Elcelina Rosa Silva

Redes Universitárias
Segurança e Auditoria

O caso das Instituições de Ensino Superior em Cabo Verde

Universidade Jean Piaget de Cabo Verde

Campus Universitário da Cidade da Praia
Caixa Postal 775, Palmarejo Grande
Cidade da Praia, Santiago
Cabo Verde

2.10.06

Elcelina Rosa Silva

Redes Universitárias
Segurança e Auditoria

O caso das Instituições de Ensino Superior em Cabo Verde

Universidade Jean Piaget de Cabo Verde

Campus Universitário da Cidade da Praia
Caixa Postal 775, Palmarejo Grande
Cidade da Praia, Santiago
Cabo Verde

2.10.06

Elcelina Rosa Correia Silva, autora da monografia intitulada Redes Universitárias – Segurança e Auditoria, declaro que, salvo fontes devidamente citadas e referidas, o presente documento é fruto do meu trabalho pessoal, individual e original.

Cidade da Praia aos 20 de Setembro de 2006
Elcelina Rosa Correia Silva

Memória Monográfica apresentada à Universidade Jean Piaget de Cabo Verde como parte dos requisitos para a obtenção do grau de Licenciatura em Engenharia de Sistemas e Informática.

Sumário

Este trabalho de investigação apresenta a problemática das Redes Universitárias cujo objectivo principal é perceber o panorama da Utilização das Novas Tecnologias, Segurança e Auditoria nas Instituições de Ensino Superior em Cabo Verde.

As técnicas utilizadas para a atingir os objectivos do mesmo, foram consultas de obras bibliográficas, distribuição e análise de dois questionários para o estudo do caso prático.

Como resultado da pesquisa surgem alguns indicadores que caracterizam o nível da utilização das Tecnologias de Informação e Comunicação nas Instituições de Ensino Superior em Cabo Verde e o estado da implementação da segurança de informação nessas instituições.

Agradecimentos

À minha mãe e a todos os meus irmãos pelo imenso carinho e protecção que têm por mim.

À Neneth, Gilberto e Gilbertinho, por todos os anos de convivência, agradeço o apoio prestado à minha educação durante uma fase fundamental para a formação da minha personalidade.

Ao Odair Varela, pela paciência, amizade e cuidado mostrados nos momentos de maior dificuldade na execução deste trabalho.

Meus agradecimentos especiais aos meus professores, em particular ao meu orientador Mestre Isaías Barreto da Rosa pela orientação, e aos colegas do curso pelos conhecimentos que partilharam comigo e que contribuíram para a minha formação pessoal.

À minha família, obrigada pelo vosso carinho.

Conteúdo

Introdução 12

1.1 Enquadramento 12
1.2 Objectivos 13
1.3 Metodologia 14
1.4 Estrutura do Trabalho 14

Capitulo 1 : A Universidade e as Novas Tecnologias 16

1.1 O conceito da Universidade 16
1.2 A Universidade face ao Impacto das Novas Tecnologias 22
1.3 O Ensino Universitário Face às Exigências Tecnológicas 25
1.4 Os Conceitos Actuais de Universidades 26
1.4.1 A Universidade «Tradicional» 26
1.4.2 A Universidade Digital 27
1.4.3 A Universidade Virtual 28

Capitulo 2 : Redes Universitárias 30

2.1 Redes Universitárias 30
2.1.1 Utilizadores de Redes Universitárias 32
2.1.2 Topologia Física de uma Rede Universitária 34
2.1.3 Requisitos de uma Rede Universitária 36
2.2 Componentes das Redes Universitárias 38
2.2.1 Tecnologias de Redes 38
2.2.1.1 Os Recursos da Rede Física 38
2.2.1.2 Redes sem fio 41
2.2.1.3 Virtual LANs 42
2.2.1.4 Virtual Private Network 44
2.2.1.5 Gestão das Redes Universitárias 45
2.2.2 Gestão Académica e Tecnologias de Ensino 47
2.2.2.1 Portal Universitário 47
2.2.2.2 Sistemas de Informação Académico 50
2.2.2.3 Biblioteca Digital 54
2.2.2.4 Ensino à Distância 55

Capitulo 3 : A Segurança Informática 57

3.1 Aspectos Históricos 57
3.2 Conceito da Segurança 59
3.3 Tipos da Segurança Informática 60
3.3.1 Segurança da Informação 60
3.3.2 Segurança Física 61
3.3.2.1 Segurança do Pessoal 61
3.3.2.2 Segurança das Instalações 63
3.3.2.3 Segurança do Equipamento 63
3.3.3 Segurança Lógica 64

3.3.3.1 Gestão do Sistema Informático e da Rede 65
3.3.3.2 Segurança dos Sistemas Aplicacionais 67
3.3.3.3 Gestão e controle de Acessos 68
3.4 A segurança nas Redes Universitárias 70

Capitulo 4 : A Auditoria Informática 73

4.1 Aspectos Históricos 74
4.2 Objectivo da auditoria 75
4.3 Tipos de auditoria 76
4.4 A Auditoria Informática 79
4.4.1 Tipos de Auditoria Informática 80
4.4.2 Porquê Auditar 81
4.4.3 Finalidade da Auditoria Informática 83
4.4.4 Relações da auditoria informática e o controlo Interno 83
4.4.5 Características do Auditor Informático 84
4.4.6 Principais técnicas de Análise e de Controlo 85

Capitulo 5 : O caso das Instituições de Ensino Superior em Cabo Verde 87

5.1 Enquadramento 87
5.2 Caracterização da Amostra 89
5.3 Análise dos Resultados 91
5.3.1 A Utilização das Tecnologias de Informação E Comunicação 91
5.3.1.1 As Infra-Estruturas de Rede 91
5.3.1.2 Tecnologias de Informação e Comunicação 93
5.3.1.3 Taxa de utilização dos Recursos 95
5.3.1.4 Tecnologias para o Ensino Universitário 97
5.3.2 Estado da Segurança da Informação 100
5.3.2.1 O Sistema de Gestão das Redes 100
5.3.2.2 Práticas da segurança e Auditoria da informação. 102
5.3.2.3 Implementação das Políticas de Segurança 104
5.3.2.4 Estado da implementação de Algumas Práticas para a Segurança. 106
5.3.2.5 Sensibilidade em relação à utilização das TICs e à Segurança da Informação 108
5.3.2.6 Que Perspectivas de Inovações Tecnológicas 109
5.3.3 Desafios e Potencialidades 110

Conclusão 112

Bibliografia 119

Anexos 124

Questionário 1 124
Questionário 2 124

Figuras

Figura 1 – Organigrama da Universidade Jean Piaget de Cabo Verde 18
Figura 2 – Universidade Técnica de Lisboa 19
Figura 3 - Estrutura de uma Rede Universitária 35
Figura 4 - Estrutura da Rede Física Universitária 39
Figura 5 - Recursos da Rede Física 40

Gráficos

Gráfico 1 - Instituições de Ensino Superior em Cabo Verde 89
Gráfico 2 - Infra-estrutura da Redes nas Instituições 92
Gráfico 3 - Estatística do número de Utilizadores, Computadores e Servidores 94
Gráfico 4 - Taxa de existência de alguns Recursos para o Ensino 98
Gráfico 5 - Forma de funcionamento dessas instituições 100
Gráfico 6 - Pessoal de Administração e Gestão das Redes 101
Gráfico 7 - Estado da Segurança Global das Instituições 102
Gráfico 8 - Controlo e Gestão de Acesso 103
Gráfico 9 - Auditoria das Redes 104
Gráfico 10 - Políticas de segurança 105
Gráfico 11 - Nível da sensibilidade dos administradores sobre a segurança 108
Gráfico 12 - Sensibilidades em relação à formação de utilizadores e novas tecnologias 110

Tabelas

Tabela 1 - Tipos de ligação e larguras de banda.....92
Tabela 2 – Estatística de alguns Recursos da Rede.....94
Tabela 3 – Avaliação da Taxa de acesso de alguns recursos tecnológicos.....96
Tabela 4 – Avaliação da taxa de utilização dos recursos disponibilizados na rede.....97
Tabela 5 - Implementação de algumas políticas de segurança.....105
Tabela 6 - Implementação de algumas práticas de Segurança.....107
Tabela 7 - Inovação Tecnológica.....109
Tabela 8 - Avaliação de alguns indicadores por parte dos inquiridos.....111

Introdução

1.1 Enquadramento

A Internet e a utilização das Tecnologias de Informação e Comunicação têm provocado uma mudança significativa nos comportamentos, nas posturas das pessoas e na forma como as organizações oferecem os seus bens e serviços.

A evolução tecnológica e a propagação da utilização das novas tecnologias e redes informáticas obrigam as organizações a um processo de constantes reajustes às tecnologias que utilizam, o que, naturalmente, condiciona maiores sensibilidades na gestão e segurança da informação e, por conseguinte, na segurança Informática.

As Universidades, como instituições de Ensino Superior, tendo como duas das suas principais funções o Ensino e a Investigação, não podem escapar a esta senda da Digitalização, constituindo-se como instituições de grande responsabilidade na construção da sociedade do conhecimento e na preparação da sua comunidade para os desafios tecnológicos face ao propalado fenómeno da globalização.

Para as Universidades, a utilização das Novas Tecnologias é essencial para garantir a Segurança das Informações e das Tecnologias de Informação e Comunicação, de modo a proteger a reputação e a segurança da investigação científica e dos valores intelectuais da mesma.

Em Cabo Verde, muito pouco se sabe do estado da Utilização e da Segurança das Tecnologias de Informação e Comunicação nas Instituições de Ensino Superior no país, na medida em que não se encontram disponíveis estudos nesse domínio. É neste contexto que o presente trabalho de investigação se enquadra, apresentando a problemática das Redes Universitárias, Segurança e Auditoria informática, a partir de um estudo de caso que incide sobre a realidade das redes das Instituições de Ensino Superior neste Estado.

A escolha deste foi motivado pelo interesse em conhecer o estado da utilização das Tecnologias de Informação e Comunicação nas Instituições de Ensino Superior em Cabo Verde e as suas tendências futuras motivadas pelos progressos tecnológicos, uma vez que actualmente as novas tecnologias constituem-se num requisito fundamental para um ensino de qualidade e por permitirem um acesso privilegiado às informações extravasando os limites geográficos e temporais.

1.2 Objectivos

Os **objectivos gerais** deste trabalho de investigação são:

- Compreender a segurança e auditoria de redes de computadores e as suas especificidades nas redes universitárias,
- Perceber o panorama da segurança e auditoria no contexto das instituições de ensino superior em Cabo Verde.

Os **objectivos específicos** são:

- Entender a estrutura da Rede nas instituições de ensino em Cabo Verde;

- Estudar a utilização das Tecnologias de Informação e Comunicação nessas instituições;
- Analisar algumas práticas de Segurança da Informação;
- E, inteirar-se da sensibilidade dos administradores de rede em relação às tecnologias de informação e comunicação e à segurança da informação.

1.3 Metodologia

As técnicas utilizadas para a concretização deste trabalho são:

- Consulta de obras bibliográficas.
- Distribuição de 2 questionários em 5 das 6 instituições de ensino existentes no país, ocorrida em duas fases, com o intuito de explorar os conhecimentos adquiridos em segurança e auditoria informática.
- Análise e tratamento dos dados recolhidos.

O estudo teve como **perguntas de partida**:

- Qual é a importância e o contributo das Novas Tecnologias, numa Instituição do Ensino Superior?
- Quais são as tendências da utilização das Tecnologias de Informação e Comunicação e as práticas da segurança e auditoria da informação nas instituições de Ensino Superior em Cabo Verde?

1.4 Estrutura do Trabalho

Este trabalho tem a seguinte estrutura:

A **introdução** onde se faz referência ao tema do trabalho, aos objectivos gerais e específicos, às perguntas de partida, à metodologia utilizada, e a um breve resumo de todos os capítulos do trabalho.

No primeiro capítulo, **A Universidade e as Novas Tecnologias,** aborda-se os conceitos básicos de Universidade, da sua estrutura orgânica e da composição da comunidade académica. Fala-se do impacto das Novas Tecnologias nas Universidades e as tendências do ensino universitário face às exigências tecnológicas. E, finalmente, incide-se sobre os conceitos de Universidade Tradicional, Digital e Virtual.

No segundo capítulo – **Rede Universitária**, fala-se da rede universitária e das suas características ao nível de estruturas, requisitos e utilizadores. Aborda-se também as componentes das redes universitárias no que concerne às tecnologias de rede, gestão académicas e tecnologias de ensino.

No terceiro capítulo – **A Segurança Informática**, faz-se a referência aos seus conceitos básicos, à segurança a nível físico e lógico, e, na parte final, à questão da segurança nas Redes Universitárias.

No quarto capítulo, **A Auditoria Informática**, faz-se alusão aos conceitos básicos da auditoria, dos vários tipos da auditoria informática e das principais técnicas da auditoria informática.

No quinto capítulo, **O Caso das Instituições de Ensino em Cabo Verde**, começa-se, primeiramente, por se fazer o enquadramento do estudo e a caracterização da amostra. Depois procede-se à análise dos dados em duas fases: Num primeiro momento analisa-se a existência e a taxa de utilização das TIC (Tecnologias de Informação e Comunicação) nas instituições em questão, bem como as tecnologias utilizadas para processo de ensino-aprendizagem. Num segundo momento analisa-se, igualmente, o estado da segurança da informação nessas instituições mediante o estudo de indicadores como o sistema de gestão das redes, as políticas e as práticas de segurança implementadas nessas instituições, assim como a sensibilidade dos administradores de rede em relação às novas tecnologias e a segurança da informação.

E, finalmente na conclusão, faz-se o remate do trabalho, recorrendo a observações recomendações em relação aos resultados alcançados.

Capitulo 1 : A Universidade e as Novas Tecnologias

1.1 O conceito da Universidade

A *Magna Charta Universitatum*, proclamada em Bolonha a 8 de Setembro de 1998, define que, no seio das sociedades diversamente organizadas e em virtude das condições geográficas e do peso da história, a Universidade é "*uma instituição autónoma que, de modo crítico, produz e transmite a cultura através da investigação e do ensino*"[1].

Uma universidade é uma instituição de ensino e de formação profissional que tem como objectivo principal a formação das pessoas e a investigação nas diversas áreas do saber, com o intuito de criar e actualizar conhecimentos. É uma instituição de educação superior, com concessão de graus académicos, que provê educação tanto ternária (graduação) quanto quaternária (pós-graduação).

A razão de ser da universidade é a criação e a descoberta da informação (através da pesquisa), a sua transmissão (através do ensino e das actividades de extensão) e o seu registro (através da produção de publicações que são colectadas em bibliotecas), (Imre, 1997).

[1] www.cnaves.pt

A palavra Universidade surgiu da palavra Latina "*universitas*" que significa corporação de estudantes. A primeira Universidade surgiu na época medieval "*University of Magnaura*", fundada em 849, na Constantinopla no Istambul - Turquia, pelo imperador Michael III[2].

As universidades normalmente têm um presidente que está no topo hierárquico, designado por Reitor, depois vem um vice-presidente ou vice-reitor e um conjunto de divisões. Estas estão subdivididas em departamentos, escolas ou faculdades e podem estar geograficamente separadas.

Podem as universidades ser públicas ou privadas. As públicas tem uma entidade do governo, por exemplo, o "Ministério da Educação", que está hierarquicamente acima da gestão universitária, que aprova planos curriculares de cursos além de controlar e suportar todo o custo financeiro. Nas privadas, os custos financeiros das universidades são inteiramente suportadas pelas mesmas.

Apesar de existir inúmeras diferenças culturais, económicas ou mesmo estruturais entre as universidades, estas são importantes para o desenvolvimento dos países onde estão instaladas, por contribuir para a formação e cultura das pessoas e da sociedade, mediante a educação dos indivíduos e pesquisas que, sobretudo, contribuem para o progresso económico e tecnológico, aspectos importantes para o desenvolvimento de um país.

Nas universidades existem a comunidade de alunos, docentes e funcionários e, além de existirem cursos nas mais variadas áreas de investigação, também existem lugares cruciais para o bem-estar da sua comunidade tais como as bibliotecas, uniões académicas, hospitais e clínicas universitárias, laboratórios de informática, de investigações, incubadoras de negócio, centros de desporto, restaurantes, bancos, lojas, centros de trabalho e de entre outros.

As universidades, tal com a generalidade das organizações de trabalho, têm um organigrama, que varia de universidade para universidade, porque este é baseado em aspectos como: o país onde está instalada; se é pública ou privada; anos de existência; número de alunos, de faculdades, de cursos; e o próprio ambiente e contexto em que a universidade vive. Assim, em caso de instabilidades internas e externas, podem ser reestruturadas de modo a

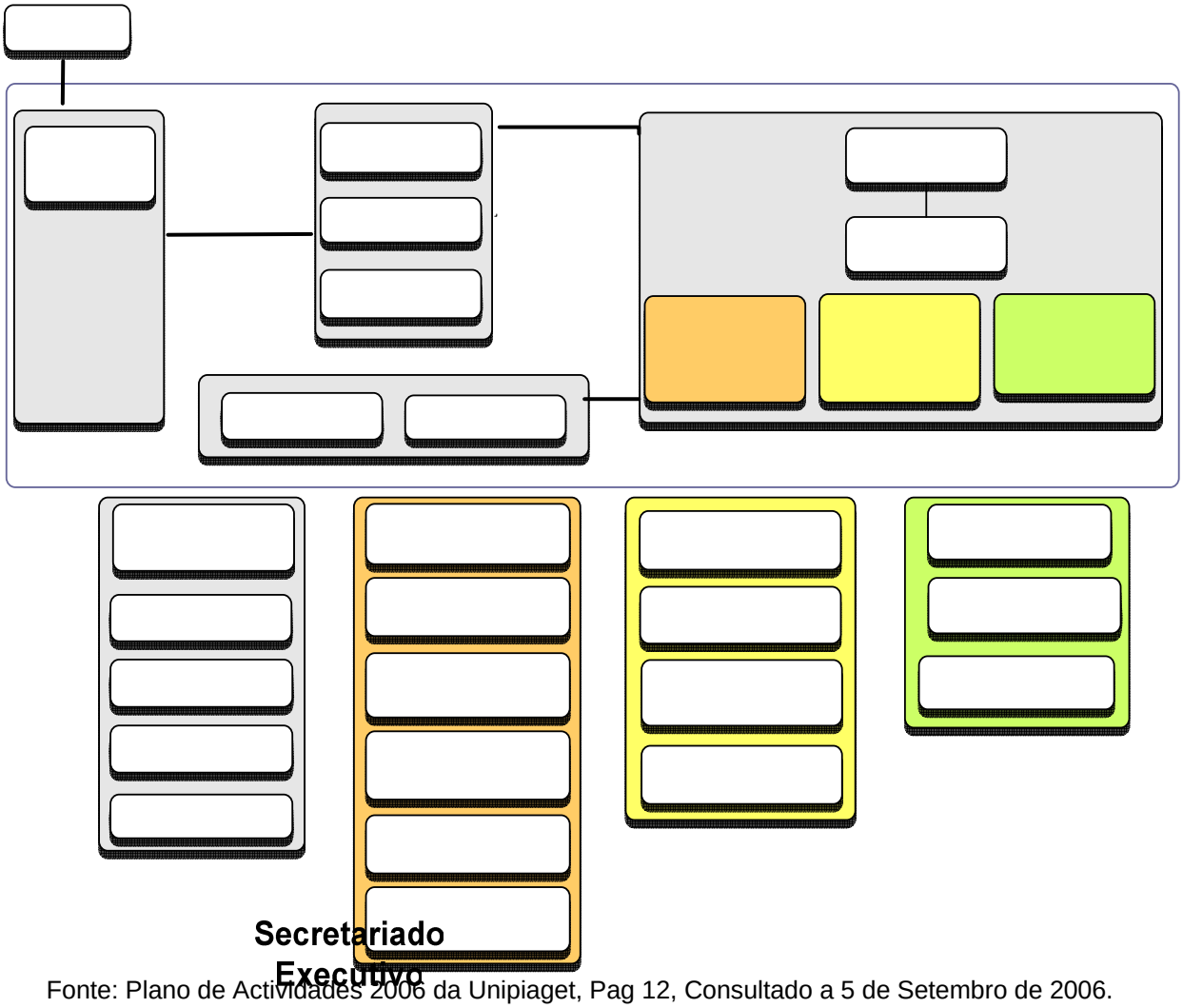
[2] http://pt.wikipedia.org

garantir um normal funcionamento das actividades académicas que são essencialmente o ensino, a investigação e as actividades da extensão universitária.

A universidade é uma instituição onde existem pessoas enquadradas em diversas categorias tais como: Pessoal Docente e Investigador; Pessoal Não Docente (Funcionários); e Alunos dos diversos cursos de graduação, pós-graduação e de formação profissional.

Numa consulta a organigramas universitários, observou-se que as universidades têm uma estrutura hierárquica que varia de universidade para universidade, de País para País, ou mesmo se é pública ou privada. As figuras que se seguem mostram dois organigramas, seleccionados dos diversos encontrados ao longo da pesquisa, fazendo referência à estrutura orgânica da Universidade Jean Piaget de Cabo Verde e da Universidade Técnica de Lisboa (Portugal).

Figura 1 – Organigrama da Universidade Jean Piaget de Cabo Verde

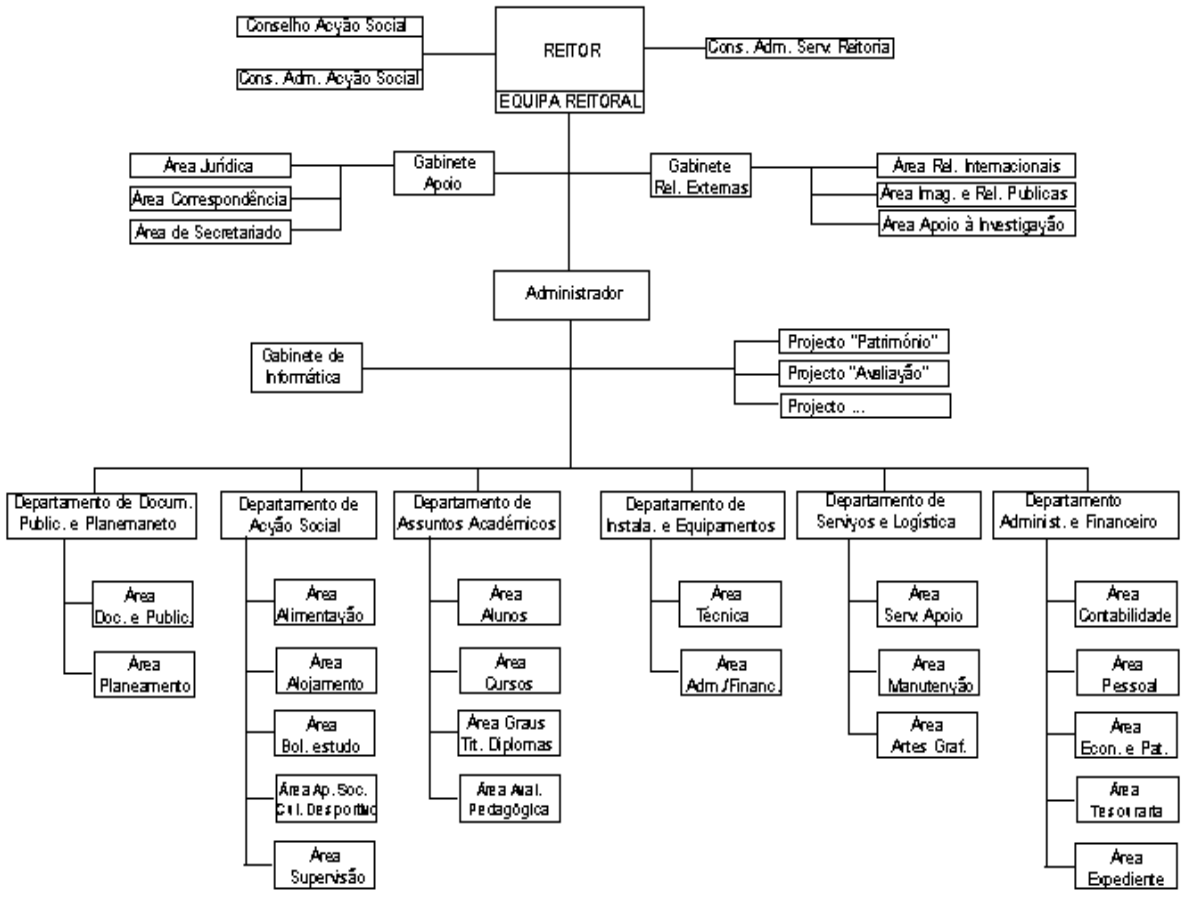


Fonte: Plano de Actividades 2006 da Unipiaget, Pag 12, Consultado a 5 de Setembro de 2006.

A Universidade Jean Piaget de Cabo Verde tem 5 anos de existência, foi fundada a 7 de Maio de 2001. Actualmente dispõe de aproximadamente 1420 alunos distribuídos por 16 cursos de licenciaturas e 4 de pós-graduação. Conta com aproximadamente 168 docentes e 80 funcionários.

A sua estrutura orgânica é composta pela Reitoria e pela Administração Geral. A Administração tem a seu cargo a Gestão Administrativa e a Reitoria a Gestão dos Serviços Académicos. No organigrama pode-se constatar que existem 3 conselhos (Consultivo, Disciplinar e Geral) que estão tutelados tanto pela Administração Geral como pela Reitoria e mais dois concelhos (Científico e Pedagógico) que estão apenas sobre a tutela da Reitoria. Existem quatro Unidades, cinco Gabinetes, três Institutos, dois Departamentos, três serviços e uma Divisão, que estão tutelados tanto pela Reitoria como pela Administração Geral.

Figura 2 – Universidade Técnica de Lisboa



Fonte: http://www.sas.utl.pt/info/Organi.htm, 2 de junho de 2006

A Universidade Técnica de Lisboa (**UTL**), foi criada em 1930, dispõe de faculdades criadas a partir de quatro escolas anteriormente existentes:

1. A Escola Superior de Medicina Veterinária, actual Faculdade de Medicina Veterinária (FMV),
2. O Instituto Superior de Agronomia (ISA),
3. O Instituto Superior de Ciências Económicas e Financeiras, actual Instituto Superior de Economia e Gestão (ISEG) e,
4. O Instituto Superior Técnico (IST).

Posteriormente, esta universidade passou a contar com três novos estabelecimentos de ensino superior: o Instituto Superior de Estudos Ultramarinos, em 1961, actual Instituto Superior de Ciências Sociais e Políticas (ISCSP), o Instituto Superior de Educação Física, em 1976, actual Faculdade de Motricidade Humana (FMH) e a Faculdade de Arquitectura (FA), em 1979.

A UTL, tem aproximadamente 19.620 alunos de licenciatura e 2.100 de mestrado, são ministrados 50 cursos de licenciatura, 88 de mestrado, 49 áreas de doutoramento, 42 pós-graduações que não conferem grau, e 2 cursos de especialização[3].

Nesta Universidade, de acordo com o organigrama, observou-se a existência de um órgão máximo que é a Reitoria. Esta é composta por Conselhos, Gabinetes e Administração. Em relação aos conselhos encontrámos: o Conselho de Administração dos Serviços da Reitoria; o Conselho da Acção Social e da Administração da Acção social. Nos Gabinetes temos os Gabinetes das Relações Externas e de Apoio e na Administração, Gabinetes de Informática, de Projectos e 6 Departamentos com diferentes funções.

Do que foi referido podemos reconhecer que a Universidade Técnica de Lisboa é uma universidade pública com muita experiência na área do ensino investigação e extensão universitária, enquanto que a Universidade Jean Piaget de Cabo Verde por ter sido criado,

[3] http://www.utl.pt/

Apenas há cinco anos conta com menos experiência enquanto Instituição de Ensino Superior universitário.

Observando os organigramas das duas universidades, pode-se constatar que na Universidade Jean Piaget de Cabo Verde (Unipiaget), a Reitoria e a Administração Geral estão no Topo da Hierarquia do poder de decisão, enquanto na Técnica de Lisboa (UTL) a Reitoria é o órgão Máximo na tomada de decisões. Uma outra diferença entre os dois organigramas prende-se com o facto da Reitoria da Unipiaget ser composta por três Pró-Reitores, enquanto que na UTL a Reitoria funciona como uma equipa constituída por Concelhos, Gabinetes e Administração.

A Unipiaget não tem Faculdades mas sim Unidades e estas Unidades funcionam à semelhança de Faculdades. Uma outra diferença entre a Unipiaget e a UTL é a existência de um departamento chamada de Departamento de Acção Social, que trata de assuntos de alojamento e atribuição de bolsas aos estudantes, o que não existe na Unipiaget, por ser uma universidade privada.

No que toca a semelhanças entre essas duas instituições, ambas detêm uma comunidade de alunos, docentes e funcionários, o que torna a universidade num espaço onde existem pessoas com perfis e funções diferentes, influenciando, assim, a estrutura e os requisitos das redes universitárias.

Esta comparação, tem como objectivo mostrar que duas instituições de ensino superior podem não ter organigramas iguais, mas deverão ter em comum três aspectos fundamentais: Ensino, Investigação e Extensão Universitária. Isto quer dizer que independentemente da sua estrutura de funcionamento interno, devem funcionar o ensino, a investigação e a extensão Universitária.

> Segundo Lamas, “o papel da educação é determinante para o desenvolvimento humano. Importa, pois, que a Universidade esteja estruturada de forma a poder responder aos desafios que de dentro ou de fora que lhe são lançados. Só assim poderá em paralelo garantir uma formação educacional de qualidade, proporcionar condições para uma aprendizagem profissional, para o crescimento pessoal e intelectual de quem

procura os seus serviços. Permitirá, desse modo, uma produtividade académica de alto nível, a construção de competências profissionais e o desenvolvimento de atitudes que viabilizam a inserção do indivíduo na sociedade do século XXI, na sociedade do conhecimento" (2006).

1.2 A Universidade face ao Impacto das Novas Tecnologias

A revolução das Tecnologias da Informação, iniciada nos anos 70 nos Estados Unidos, teve profundas implicações em inúmeros sectores da sociedade, e desde logo na forma como os sujeitos interagem entre si, diversos autores falam mesmo na perda da relevância do espaço físico ou do lugar, (Antunes, 2001).

Segundo Rodrigues (2004), as "**Novas Tecnologias**" são a reunião dos meios audiovisuais, informáticos e de comunicação que permitem criar, armazenar, recuperar e transmitir informações a grande velocidade e em grandes quantidades.

Actualmente depara-se com uma grande facilidade de acesso às tecnologias de informação e comunicação, influenciada pela forte miniaturização dos equipamentos informáticos, pelos preços cada vez mais acessíveis desses equipamentos, bem como pela diminuição do custo da comunicação. Cada vez mais as pessoas e as organizações de diversos tipos utilizam essas tecnologias no sentido da obtenção e garantia de vantagens competitivas, principalmente no seio das chamadas sociedades modernas. Isto contribui para a emergência de uma nova postura por parte das escolas, das organizações e da sociedade.

Caminha-se para uma Sociedade da Informação e do Conhecimento. Esta sociedade caracteriza-se, fundamentalmente, pela substituição da mão-de-obra e da energia pela informação, que funciona como força motora do desenvolvimento da economia e de todos os sectores de actividade, (Rodrigues, 2004). Segundo este autor, a Sociedade do Conhecimento resulta do desenvolvimento das auto-estradas da informação e tem um enorme impacto nos indivíduos e nas organizações. É responsável por mudanças significativas na economia, nos padrões do comportamento social e é marcada pelo domínio da informação decorrente das

Tecnologias de Informação e Comunicação. Deriva da convergência entre a informática, as telecomunicações, o audiovisual, a telemática e a multimédia.

Na perspectiva de Roberto Carneiro (2001), apud (Oliveira, 2005), dois tipos de consequências educativas podem ser tiradas dessas novas tecnologias, destacando:

- A necessidade de educar para a sociedade da informação numa dupla vertente: formação dos jovens e a actualização e reciclagem de adultos;
- A urgência de repensar o modelo pedagógico em aplicação nos estabelecimentos de ensino à luz dos novos e diferentes modos de pensar.

Um dos desafios contemporâneos enfrentados pelas escolas, na perspectiva de (Melo et all, [S/D]), é o de garantir o desenvolvimento de todos os seus alunos, no interior de grupos cada vez mais heterogéneos. Num contexto de ensino, é indispensável pensar em novas ferramentas pedagógicas (Tecnologias Educativas) que permitam responder às necessidades de ensino e aprendizagem, de actualização e produção do conhecimento, bem como de uma maior eficiência de comunicação entre alunos e professores.

As novas tecnologias devem ser utilizadas na prespectiva de (Figueiredo, 2000), em função das exigências actuais da aprendizagem e não em função dos paradigmas do passado. Este autor defende que, é importante considerar a necessidade de criar contextos de aprendizagem, interacções e ambientes sociais culturalmente ricos proporcionados pela utilização da tecnologia e de ambientes de aprendizagem baseados na Internet, porque a utilização destas tecnologias tornam-se cada vez mais indispensáveis na organização curricular da aprendizagem.

Uma sociedade em constante mudança coloca um permanente desafio ao sistema educativo. As TIC estão, cada vez mais, presentes na actividade profissional dos docentes. A nova e principal função destes deve residir no facilitar o acesso ao conhecimento e, tendo em conta que as novas tecnologias permitem realizar esta função, pode-se falar de um novo paradigma educacional Riço (2002), apud (Rodrigues, 2004).

O professor, mais que uma fonte absoluta de saber e ciência, transforma-se no incentivador da aprendizagem na sala de aula e além de dominar os conteúdos que pretende ensinar, ele precisa promover a interacção entre os participantes do processo e indicar meios para a aproximação, por parte dos mesmos, das fontes nas quais podem encontrar os subsídios necessários para a construção do conhecimento. Conhecimento este, aliás, em constante mudança, que vai para além de qualquer conceito de estabilidade, permanentemente reconfigurado e reconstruído, disponível em uma multiplicidade de meios e fontes, num contexto de mediação tecnológica jamais visto anteriormente, em termos históricos. Neste caso para mudar, a "**sala de aula**", este, precisa ser um espaço que transcende os limites institucionais, (Oliveira, 2005).

A grande influência das TIC na Universidade acarreta consigo a necessidade da adequação das instituições de Ensino Superior a uma realidade em que essas tecnologias têm um papel determinante em todos os aspectos de vida organizacional. As tecnologias de informação e de comunicação tornaram-se numa ferramenta básica para a maioria das universidades, enquanto que a demanda e as expectativas dos utilizadores aumentam a cada dia (Moul, 2003).

Sendo a universidade uma organização que dispõe duma comunidade relativamente numerosa e complexa em termos das necessidades de utilização dos recursos tecnológicos, visto que existem docentes de várias categorias e áreas científicas, funcionários com diversas funções e alunos de diferentes cursos, há que ter algum domínio da utilização das novas tecnologias, de modo a acompanhar os novos desafios e exigências que surgem a cada dia, de forma a garantir que o processo de ensino-aprendizagem tenha qualidade. Levando em consideração que as comunidades de alunos, docentes e funcionários têm as suas especificidades no que respeita às exigências da utilização dos recursos tecnológicos para desempenharem as suas funções, há que ponderar a distribuição desses recursos para que todos na universidade possam produzir e desenvolver intelectualmente. Neste caso, para garantir que todos tenham acesso às tecnologias que precisam para a aprendizagem e pesquisa, há que acompanhar a evolução tecnológica no sentido amplo do termo.

1.3 O Ensino Universitário Face às Exigências Tecnológicas

As Novas Tecnologias de Comunicação e Informação criaram oportunidades sensíveis a mudanças nas relações de poder, principalmente no convívio aluno (s) - professor (es), e ampliaram os locais e os tempos de aquisição de saberes e competências, antes restritos ao espaço/tempo, hoje para além da sala de aula e suas extensões tradicionais, (Oliveira, 2005).

A construção dos conhecimentos necessários para a aquisição das competências almejadas para os estudantes dos cursos universitários passa, inevitavelmente, pela mudança deste quadro, de maneira a engajar o aluno como elemento activo, crítico e autónomo. Não mais o «assimilador passivo de conteúdos», mas sim o construtor do próprio aprendizado, alguém que interfere na trajectória que lhe diz respeito, ajusta roteiros aos interesses, habilidades, capacidades, disponibilidades e realidades, (Oliveira, 2005).

Actualmente, com a Internet a informação e a troca de conhecimento e de experiências é cada vez mais visível no seio das comunidades académicas, influenciando assim o aparecimento das chamadas comunidades virtuais. A aprendizagem, a qualificação técnica e o acesso ao saber, caminha para ser algo flexível, não voltado ao espaço físico com um professor mas sim para ambientes virtuais. Comunidades virtuais de aprendizagem são estruturadas a partir de cursos/disciplinas oferecidas em modo semi-presencial ou à distância. Entretanto, tais comunidades extrapolam os tempos rígidos marcados para a duração de um curso. As pessoas desejam continuar conectadas a esses ambientes, mantendo a aprendizagem permanente, preservando objectivos e buscando resultados comuns, participando de forma igualitária, trabalhando em equipa, aprendendo colaborativamente e interagindo permanentemente. Aqui, professores são «orientadores» e/ou «animadores», Kenski (2001) apud (Oliveira, 2005).

Novos desafios que surgem para as universidades no que concerne à pesquisa e ensino, sendo que as comunidades virtuais vêm contribuindo, de forma permanente, para o surgimento das chamadas Universidades Virtuais, devido às vantagens que esta apresenta nomeadamente: o desaparecimento das barreiras geográficas; a partilha de experiências e recursos; a facilidade no acesso à informação; a diminuição de processos burocráticos e de custos.

Nesta óptica, caminha-se para um novo ambiente universitário que funcionará de forma digital e/ou virtual. Para isso, muitas tarefas precisam de ser automatizadas de modo a permitir trocas de informações e saberes, num ambiente virtual. Assim as universidades que funcionam fora desse renovado ambiente universitário correm o risco de serem ultrapassadas pelas exigências tecnológicas que o mundo enfrenta e face ao surgimento de novas tecnologias.

1.4 Os Conceitos Actuais de Universidades

1.4.1 A Universidade «Tradicional»

Uma universidade «tradicional» é aquela em que todos os processos são efectuados de forma tradicional e/ou manual, não de forma automática. Nela não existe o ensino a distância pela própria filosofia de ensino tradicional, não existe a automatização nos processos de gestão.

A influência de informação que o mundo depara neste momento, a existência de universidades que funcionam de forma essencialmente tradicional é considerada quase inaceitável tendo em conta o próprio fundamento daquilo que é a Universidade.

James Clifford Taylor[4], numa palestra sobre "Tecnologia em EAD" na Universidade em Southern Queensland, afirmou que "*Se as universidades não mudarem, não sobreviverão no futuro*". A afirmação feita por este professor é baseada na sua convicção de que actualmente, na era da Internet, o conhecimento deve ser fluido, rápido e flexível. E isso, segundo ele, é tudo o que as instituições «tradicionais» não são. Ele acredita que os tempos actuais são de revolução na educação universitária, afirmando que quando passamos o ensino superior da elite para o de massas, em que a Internet constitui o factor principal. O E-learning, portanto, é a resposta. E a pergunta que ele faz é "*de que forma podemos mudar as universidades?*".

[4] Professor da Universidade de Southern Queensland nos E.U.A e investigador no domínio de Ensino à Distância na mesma Universidade, publicado no site:
http://www.universia.com.br/html/materia/materia_ccch.html

Transformar a Universidade Tradicional numa Universidade Digital e/ou Virtual, implica uma reorganização e reestruturação da forma de funcionamento, de modo a automatizar os procedimentos. Nesta óptica caminha-se para um novo ambiente universitário, que funciona em parte de forma virtual. Para isso muitas tarefas precisam de ser automatizadas de modo a permitir trocas de informações e saberes, num ambiente virtual (Rosa, 2005).

1.4.2 A Universidade Digital

A esmagadora maioria das instituições de ensino superior estão se enveredando pela senda da digitalização. Os que não o fizerem, poderão ser ultrapassados pela concorrência, (Hai,2005). Ter uma universidade que funciona de forma digital constitui actualmente numa necessidade imprescindível para as universidades ou instituições de ensino superior, tendo em conta que nos encontramos na chamada na era da informação e os avanços tecnológicos registados até esta data, exigem que as universidades também embarquem nesta revolução tecnológica de modo a garantir e sustentar a inovação do conhecimento e a construção do saber.

As Universidades digitais têm a possibilidade de oferecer uma variedade de serviços aos seus clientes com melhor qualidade, o que pode constituir-se num importante factor de diferenciação face às universidades «tradicionais». Numa universidade digital existe um pacote integrado de serviços, capacidades e práticas que permitem aos vários “clientes” da universidade comunicarem, realizarem transacções, adquirirem e fornecerem conteúdos (Losh(2002) apud (Rosa, 2005). Possibilita na perspectiva de Gatien (2000) à migração com sucesso de algumas actividades que antes funcionavam em papel, para o funcionamento em formato digital.

Criar uma Universidade Digital significa olhar a todos os processos-chave do negócio, dentro da Universidade, recriar, reintegrar e melhorar esses processos num ambiente em linha. Construir a Universidade Digital na perspectiva de Heseltine and Dolphin (2001), é uma oportunidade de reinventar os fluxos e processos do controle de informação frequentemente arcaicos para que sejam aplicáveis à actualidade das Universidades.

Segundo Heseltine and Dolphin (2001) apud (Rosa, 2005), a existência de um serviço único de acesso aos recursos e serviços disponibilizados na Universidade Digital, exige que o seu ambiente contenha vários componentes inter-relacionados, destacando:

- Intranet Organizacional, que fornece aos funcionários da universidade uma vasta panóplia de informações e recursos de modo a melhorar o seu desempenho, num ambiente em linha.
- Intranet dos alunos, provendo aos estudantes um mecanismo de acesso às informações específicas da camada estudantil e a possibilidade de efectuarem algumas operações de caracter administrativo e financeiro em linha.
- Sítio Web público, que funciona como um meio de *marketing* da universidade e da concretização da sua comunicação com uma vasta comunidade de estudantes, potenciais alunos e antigos estudantes.
- Sistema de ensino à distância, permitindo à universidade flexibilizar o processo de ensino/aprendizagem, através de um ambiente em linha que poderá eventualmente ser utilizado como um complemento ao ensino presencial.
- Biblioteca digital que fornece à comunidade universitária o acesso às publicações diversas com uma variada gama de outros recursos em formato digital, podendo estes estar acessíveis em qualquer parte do mundo, via Internet.

1.4.3 A Universidade Virtual

Uma universidade virtual não possui um *campus* Universitário, com professores, infra-estrutura física com salas de aula e bibliotecas, existindo sim um espaço de trabalho virtual funcionando de forma electrónica ou através de meios electrónicos. Na Universidade Virtual, pode-se ter um *campus* e toda uma infra-estrutura cujas operações críticas funcionam de forma automatizada. Segundo (Rosa, 2005), Quando se fala da Universidade Virtual, refere-se a uma instituição que se dedica ao ensino superior de forma virtual, ou seja, uma instituição que se dedica à educação virtual.

a Universidade Virtual, segundo Chellapa et all (1997), consiste de um corpo administrativo, instrutores, provedores de conteúdo e alunos conectados através numa infra-estrutura electrónica com mecanismos de controlo e de segurança. Nessas Universidades recolhem-se os materiais didácticos de muitos provedores de conteúdos (Bibliotecas Digitais) e de educadores.

Segundo (Rosa, 2005) a Universidade Virtual acarreta um conjunto de particularidades:

- Migração dos serviços mais importantes para o formato digital
- Integração das diversas tecnologias e serviços utilizados num único ponto de acesso permitindo o manuseamento de dados em tempo real, mesmo quando se encontrarem em sistemas distintos.
- Autenticação única do utilizador independentemente do serviço que necessite aceder.

As universidades que funcionam de forma digital têm, na perspectiva de Jones, algumas vantagens sobre as «tradicionais» (Jones; 2004), nomeadamente:

- Maior acessibilidade – as Universidades Digitais têm a possibilidade de prover oportunidades de educação a um grupo muito vasto de potenciais alunos em todas as idades e em todos os lugares do mundo, ultrapassando assim as fronteiras geográficas, sobre tudo em cursos leccionados à distância. Além de fronteiras geográficas, facilita uma maior mobilidade à comunidade académica, por estar disponível 24 horas por dia e 7 dias por semana, o que facilita a tarefa de todos os que estão de alguma forma envolvidos no processo ensino-aprendizagem.
- Auto-serviço e convergência. O portal universitário permite mecanismos de autenticação única à comunidade académica, ficando assim ultrapassados os problemas administrativos, por não se preocupar com os horários de funcionamento dos serviços administrativos da universidade, tendo em conta que estes podem ser feitos em qualquer momento através do portal.
- Partilha de recursos e ficheiros. Os recursos poderão ser partilhados não só entre os elementos integrantes da comunidade universitária mas também com outras instituição de ensinos, por exemplo, através de bibliotecas digitais.

Capitulo 2 : Redes Universitárias

2.1 Redes Universitárias

A experiência que acompanha o rápido avanço tecnológico e disseminação da informatização das actividades universitárias confirma que camadas cada vez mais amplas da comunidade universitária sentem a influência crescente das novas tecnologias nos seus afazeres diários e sentem também que, com o passar do tempo, uma porção cada vez maior das suas actividades profissionais serão afectadas pela influência transformadora dos computadores e das redes de computadores, (Imre, 1997).

Quando se fala de redes de comunicação, está-se a falar tanto de comunicação de dados como da comunicação de voz, Monteiro & Fernando (2000). Na perspectiva deste autor a rede de voz tem a ver com redes de telecomunicações, ou sistemas de telefones, e a rede de dados são as chamadas redes informáticas, utilizadas para comunicação de dados, ou de informação entre utilizadores ou sistemas computacionais dos mais variados tipos.

Segundo (Sousa, 1999) "… *Uma rede de computadores é um conjunto de equipamentos interligados de maneira a trocarem informações e compartilharem recursos, como arquivos de dados, impressoras, softwares e outros equipamentos*…"

Em quase todas as literaturas que falam das redes de dados, fazem referência a pelo menos três tipos de redes: redes de abrangência Local, Metropolitana e Mundial.

As redes de abrangência local, denominadas de ***LAN*** (***Local Area Network)***, são redes que abrangem uma área geográfica limitada como escritórios, empresas, universidades ou um conjunto de edifícios muito próximos. Devido a sua pequena abrangência, são as mais utilizadas, nela é possível interligar postos de trabalho, de modo a partilhar largura de banda, serviços disponibilizados num servidor, ficheiros, impressoras, computadores, serviços de correio electrónico e de entre outros.

As redes metropolitanas, designadas de ***MAN (Metropolitan Area Network***), são redes que interligam várias **LANs** situadas em diversos pontos duma cidade, como por exemplo, organismos governamentais, pólos universitários ou uma empresa com vários filiais.

Finalmente as ***WANs (Wide Area Network)*** ou redes de área alargada, que possibilitam a interligação de redes locais e metropolitanas dispersas por uma vasta área geográfica como um país, um ou vários continentes, possibilitando a troca e o acesso mais rápido da informação dentro das áreas interligadas.

Além destes tipos de redes existe uma rede que abrange grandes c*ampus* universitários denominada de ***Campus Area Network (CAN)***.

A ***Campus Area Network*** - define-se como uma rede que usa ligações entre computadores localizados em áreas de edifícios ou prédios diferentes, como em campus universitários ou complexos industriais e militares. Pode ser considerada uma forma de redes metropolitanas específicas para as exigências da rede académica[5].

[5] - http://pt.wikipedia.org/wiki/CAN

Em caso de serem redes de *campus* universitários, caracteriza-se por um *link* com um conjunto de c*ampus* universitário interligados que incluem faculdades, departamentos ou residências universitárias. É uma rede grande para ser considerada uma rede de abrangência Local (LAN) e pequena para ser uma rede que abranja uma área alargada (WAN).

Uma universidade caracteriza-se por um conjunto de instalações por vezes separadas geograficamente, denominadas faculdades. Estas ministram diversos cursos, contam com uma comunidade de alunos, docentes e funcionários, e com as suas especificidades em termos de exigências científico-tecnológicas para a docência e investigação, o que, cômputo geral, condiciona as necessidades de utilizações entre as diversas faculdades de recursos diferenciados.

Tendo em conta que a essência das universidades é produzir e actualizar conhecimentos que contribuam para mudanças de comportamentos, mentalidade e opiniões, há que criar condições para que isso aconteça através de meios tecnológicos, daí o surgimento das Redes Universitárias e todas as suas especificidades em termos tecnológicos.

2.1.1 Utilizadores de Redes Universitárias

As Universidades, por vários motivos, estão no centro do processo de mudanças e, por circunstâncias históricas, a comunidade académica sempre teve a oportunidade de ser o actor principal no desenvolvimento das novas tecnologias, influenciando decisivamente no estabelecimento dos novos hábitos da sua utilização. Isto porque os meios académicos serviram tanto como autores quanto como "cobaias" na criação e no estabelecimento da nova realidade que surgiu com o advento das redes de computadores (Imre,1997).

Levando em consideração que as universidades sempre estiveram no topo, em termos de utilização das tecnologias de ponta, não é fácil gerir redes universitárias porque nessas redes pode-se encontrar uma heterogeneidade de equipamentos que implicam soluções permanentes de integração.

Neste momento um dos grandes desafios das redes universitárias advém da nova forma de aprendizagem, a chamada aprendizagem colaborativa que implica necessariamente algumas reestruturações por parte das universidades no que concerne às formas de interacção professor- aluno, de acesso às informações e recursos didácticos, o que implica que as universidades acompanhem de forma severa os avanços tecnológicos de modo que não sejam ultrapassadas pela tecnologia, garantindo sempre a segurança da própria rede.

Nesta óptica e na perspectiva de (Oliveira, 2005), para que os actores envolvidos, como por exemplo, as instituições, os professores e os alunos, possam entender o papel que lhes cabe na construção do novo cenário no qual decorrerá o processo de ensino e aprendizagem, algumas questões deverão ser colocadas e respondidas, de entre as quais se destacam:

- A infra-estrutura tecnológica existente (Informação/Comunicação) é adequada e suficiente para suportar as interacções pretendidas e armazenar as informações necessárias?
- Existe um corpo técnico para dar suporte a alunos e professores, e ser capaz de resolver dificuldades relacionadas com o uso de ferramentas tecnológicas?
- O corpo docente está capacitado para utilizar as ferramentas tecnológicas?
- Cada professor está consciente ou pode ser consciencializado da relevância de sua actuação como crítico de conteúdos e métodos, orientador, proponente, tutor e como participante?
- Como fornecer aos alunos a necessária ambientalização aos novos métodos e competências necessárias para utilizar as ferramentas tecnológicas e interagir no novo contexto?
- Dispõem os alunos, em ambientes fora da universidade, de equipamentos e da infra-estrutura necessários à participação no processo que se pretende implantar? Pode a universidade suprir carências neste sentido? Como lidar com essas resistências?

Das condições enumeradas pelo autor, nota-se que o mesmo defende que o contexto em que se vive actualmente exige das escolas e, por conseguinte, das universidades alguma tecnologia que dê suporte ao novo contexto de ensino-aprendizagem, nomeadamente a infra-estrura tecnológica, pessoal técnico, alunos e docentes capacitados para utilizarem novas tecnologias bem como as condições de acesso a ambientes fora da universidade.

2.1.2 Topologia Física de uma Rede Universitária

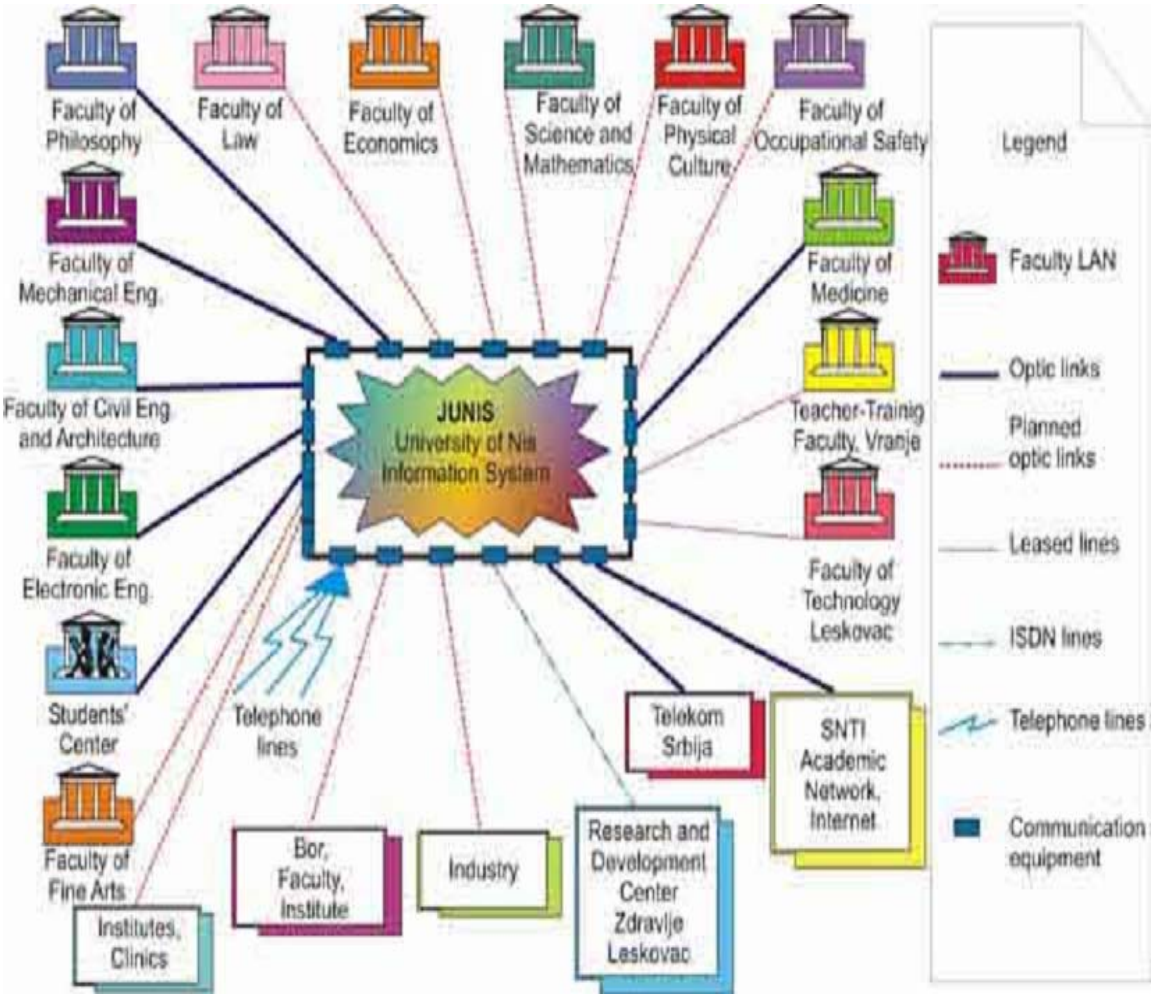
Actualmente, a utilização de novas tecnologias influencia grandemente uma rede universitária dado que, praticamente, a cada dia que passa surge uma nova tecnologia que, em diversas ocasiões, são criadas pela própria universidade, tendo em conta que esta confronta-se diariamente com novos desafios no seio da sua comunidade. Para além disso, uma universidade não deve condicionar o acesso às novas tecnologias à sua comunidade tratando-se de uma instituição voltada para a investigação e o conhecimento.

Uma universidade caracteriza-se por um conjunto de instalações por vezes separadas geograficamente, denominadas faculdades. Em cada faculdade, existem, milhares de alunos, centenas de professores e funcionários cada um com as suas especificidades, o que condiciona necessidades de utilizações diferenciados e como precisam aceder constantemente os recursos da rede, exigem que a própria rede tenha capacidades que suportem essas exigências. Geralmente, todas as faculdades têm laboratórios de informática e de investigação, unidades departamentais que exigem a utilização e actualização de novas tecnologias de informação e comunicação.

Cada faculdade tem a sua infra-estrutura física, e dentro desta destacam-se os centros de investigação, as salas de aula, os laboratórios e os departamentos. Além destes, existe a própria estrutura da rede que varia de uma faculdade para outra.

Na figura 1, pode-se observar diferentes tecnologias em termos de meios físicos de acesso. Algumas ligações de Backbone entre as diferentes faculdades são de fibras ópticas e outras são ISND, e, ainda, pode-se encontrar ligações telefónicas, o DSL e as ligações sem fio que não se encontram na figura.

Figura 3 - Estrutura de uma Rede Universitária



Fonte: www.junis.ni.ac.yu/ engleski/2332.htm, consultado a 25 de Maio de 2006

Cada faculdade pode ter uma tecnologia de transmissão de larguras de banda diferentes. Detém, igualmente, uma ligação para uma instalação central que normalmente é designada de centro de distribuição. Neste, existem diversas tecnologias Ethernet com larguras de banda diferenciadas, e vários *links* de ligação às faculdades também com larguras de banda diferenciadas. Pode-se encontrar equipamentos de rede diferenciados, em termos de variedade e de fabricação, como Roteadores, Swicthes e entre outros.

Tendo em conta que uma Universidade é uma instituição de formação, investigação e, sobretudo de produção de novos conhecimentos científicos, não se pode limitar nem padronizar a utilização de um determinado tipo de hardware e/ou software, o que explica a

razão pela qual encontra-se uma grande heterogeneidade de tecnologias nas redes universitárias.

2.1.3 Requisitos de uma Rede Universitária

Uma rede universitária é muito heterogénea porque caracteriza-se por uma diversidade de hardware e softwares, e pela exigência de serviços como o acesso à Internet, correio electrónico, acesso a base de dados e Sistemas de Informação Académico, constituindo um todo de extrema importância para o funcionamento dos serviços que garantam a produção de toda a comunidade universitária.

Muitas vezes as redes universitárias deparam-se com hardware de diversas marcas e de diferentes fornecedores, com *softwares* que funcionam em várias plataformas, por exemplo, *Linux, Mac, Windows e etc*, que exigem certas sensibilidades de integração, tendo em conta que o facto de um determinado utilizador utilizar uma determinada plataforma não justifica o não acesso a recursos a que tem direito. Neste caso, cabe à universidade criar e implementar soluções mais adequadas à sua realidade.

As universidades, dispõem duma comunidade de utilizadores bastante numerosa e complexa em termos das necessidades de utilização dos recursos, porque existem docentes de várias categorias e áreas científicas, funcionários com diversas funções e alunos de diferentes cursos. Cada comunidade (alunos, docentes e funcionários) tem a sua própria especificidade no que respeita às exigências de utilização dos recursos disponibilizados através da rede e há que ponderar, através da concepção de perfil de utilizadores, uma partilha equilibrada de recursos para que todos tenham acesso aos recursos necessários para desempenharem as suas funções, garantindo sempre a segurança lógica e física da rede. Por exemplo, dentro da comunidade de docentes estes se distribuem por diversas áreas científicas e categorias, com exigências diferenciadas ao nível do ensino e da investigação. Dado que cada área científica tem características próprias – por exemplo a área do Direito não tem as mesmas necessidades que a àrea das Ciências e Tecnlogias, a distribuição de recursos se torna num aspecto muito sensível.

Na comunidade de alunos estes também se diluem em diversas áreas científicas pertencendo a cursos diferentes e precisando de recursos diferentes para a pesquisa. Isso requer uma eficiente política de distribuição de recursos, através da definição de perfil da utilização dos recursos, de modo a que todos possam aceder aos recursos a que têm direito. Imagine uma universidade que dispõe de milhares de alunos, todos precisando aceder os recursos da Rede Universitária.

Em relação aos funcionários, estes com funções diferentes, de unidades departamentais diferentes, precisam de recursos diferenciados para executarem as suas funções. Neste cenário, há que existir mecanismos de distribuição de recursos bem delineados para que possam ter exactamente aquilo que precisam para desempenharem as suas funções.

Além das Comunidades existem ainda os laboratórios de informática destinados a diversos cursos, e que por acarretarem exigências de diferentes recursos para prática do ensino-aprendizagem, precisam de atenções especiais em termos da segurança.

Sendo a universidade uma instituição de formação e investigação é, por conseguinte, difícil padronizar a utilização de um determinado tipo de hardware e/ou software, razão pela qual encontramos equipamentos de diversas marcas e de diferentes fornecedores nas universidades. A nível de *software* também deparamos com uma variedade de opções, principalmente ao nível de sistemas operativos, o que exige uma certa integração das tecnologias utilizadas. Neste contexto, muitas vezes a concepção de perfil de utilizadores surge como a solução adoptada, dando a cada grupo de utilizadores recursos necessários para desempenharem as suas actividades. Neste caso, toma-se como referência as exigências das necessidades de cada utilizador, as particularidades de cada grupo de utilizadores, as exigências de cada unidade departamental, de modo a permitir que todos tenham acesso a recursos tecnológicos que precisam e que lhes permitem produzir dentro do contexto daquilo que é a universidade.

2.2 Componentes das Redes Universitárias

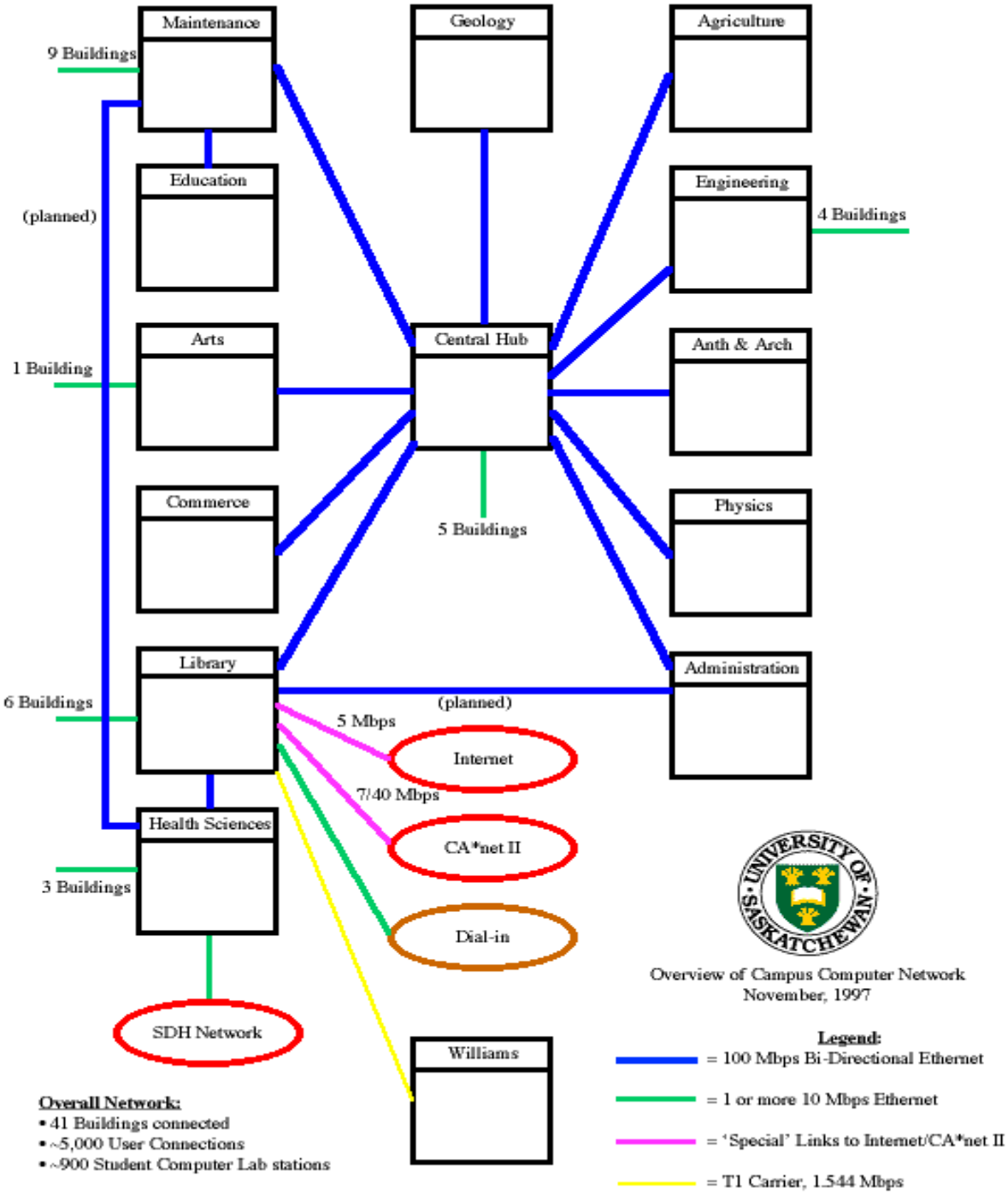
2.2.1 Tecnologias de Redes

2.2.1.1 Os Recursos da Rede Física

Numa rede universitária existem várias tecnologias de rede nomeadamente: Redes Sem Fios incorporadas dentro da rede Ethernet, Redes Locais Virtuais e Redes Virtuais Privadas, as quais far-se-á uma breve referência mais adiante. A rede universtária é composta por muitos recursos, uma variedade de *hardwares* e *softwares*, sendo, por isso, muitas vezes chamada de rede heterogénea.

Dentro da rede física, existe uma rede de utilizadores, ou seja, utilizadores com diferentes perfis de utilização dos recursos que exigem uma composição especial da rede local. Começando pelos recursos físicos, uma rede universitária dispõe de um centro de distribuição principal ou nuclear, onde encontram-se equipamentos que dão suporte ao funcionamento da rede. Nas faculdades ou escolas encontra-se os designados centros de distribuição intermediária, que se interligam ao centro de distribuição principal ou nuclear permitindo a junção de todas as faculdades ao mesmo centro, originando assim, numa única rede do *campus* – a Rede da Universidade.

Figura 4 - Estrutura da Rede Física Universitária



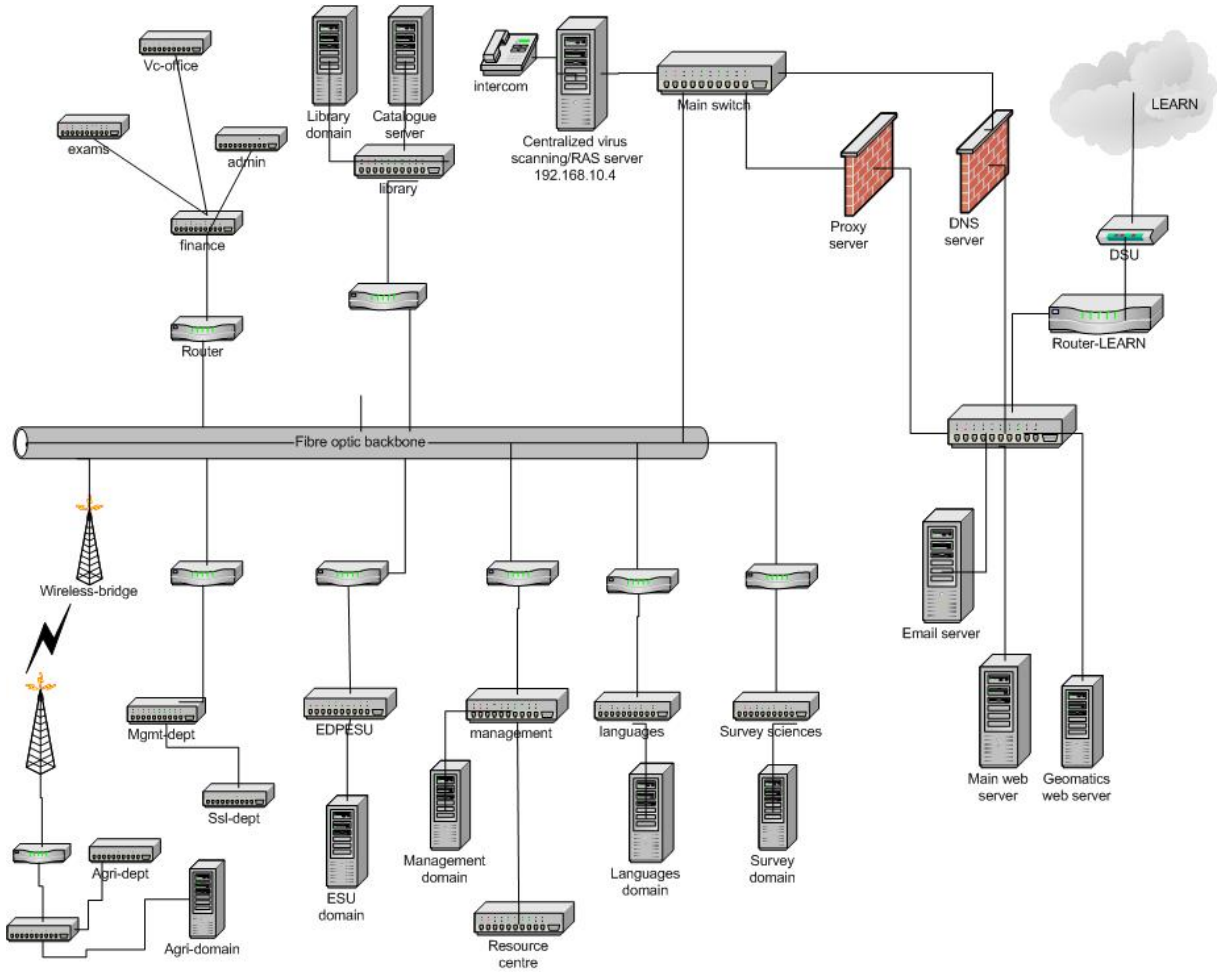
Fonte: Fonte: **www.usask.ca/.../itc/ reports/networkNov97.shtml**,

consultado a 25 de Maio de 2006

Os centros de distribuição têm equipamentos de redes como o Router e Swicth que permitem interligar computadores pessoais à rede. Além destes recursos existem as ligações físicas de diferentes larguras de banda que se interligam aos outros pontos de acesso em outras faculdades que necessitam de ser geridas.

Além desses recursos existe o acesso à Internet e os seus recursos, e os servidores de acesso nomeadamente servidores de dados, de aplicações, de e-mail, de autenticação, entre outros, que precisam de mecanismos rigorosos de autenticação e firewall funcional para a segurança dos recursos lógicos.

Figura 5 - Recursos da Rede Física



Fonte www.sab.ac.lk/ccs/, consultado a 9 de junho de 2006

Na figura enumerada em cima, pode-se constatar que nesta rede existe uma rede cabeada e uma rede sem fio incorporada dentro da rede cabeada. Além destes, existem equipamentos de redes como Router e Swicth que requerem configurações adequadas para o seu correcto funcionamento. Também pode-se observar muitos servidores com diferentes funções.

Além dos recursos que se podem observar na figura, existem os recursos lógicos nomeadamente *softwares* e dados que exigem uma gestão sensível de modo que todos podem ter dados e informações necessárias para produzir, incluindo acesso a base de informações e *softwares* específicos tendo em conta que nas universidades cada grupo de utilizadores dispõem de necessidades específicas da utilização dos recursos.

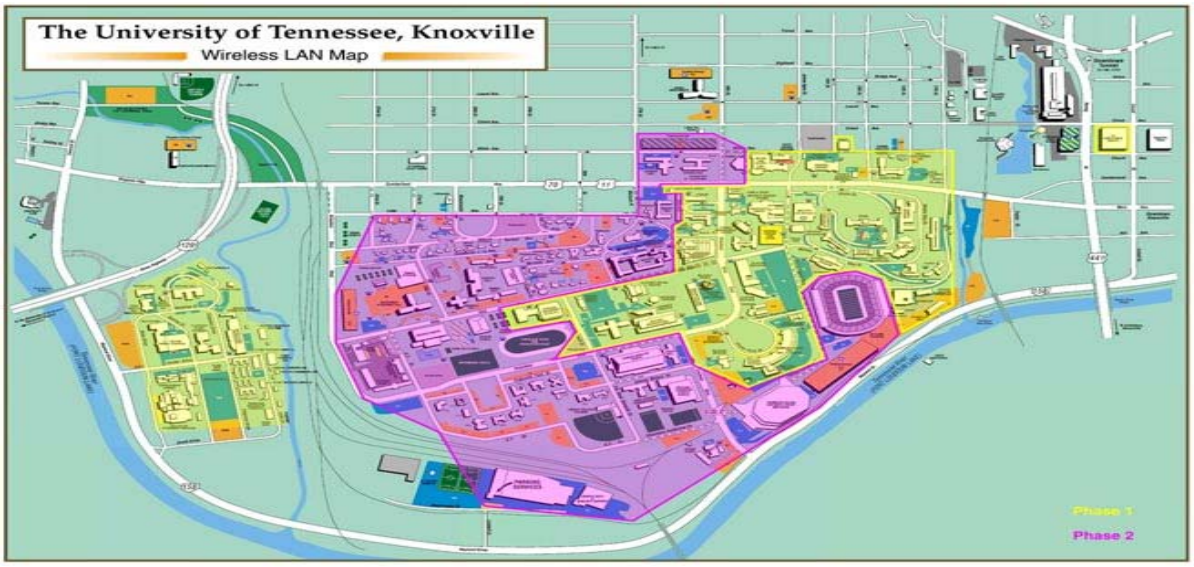
2.2.1.2 Redes sem fio

Redes Sem Fio ou "*Wireless*", como o próprio nome diz, é uma rede sem fio que usa o ar como meio de transmissão. As redes locais sem fio – *WLANs* (Wireless Local Area Network) constituem-se como uma alternativa às redes convencionais com fio (Cabeada) fornecendo as mesmas funcionalidades, mas de forma mais flexível e com boa conectividade entre prédios ou Campus.

Num ambiente típico, o dispositivo transceptor (transmissor/receptor) ou ponto de acesso (*access point*) é conectado a uma rede local Ethernet convencional (com fio). Os pontos de acesso não apenas fornecem a comunicação com a rede convencional, como também intermediam o tráfego com os pontos de acesso vizinhos. Pode-se encontrar computadores portáteis, PDAs (**P**ersonal **D**ata **A**ssistants), telefones móveis principalmente os de nova geração e algumas impressoras.

Numa rede universitária, as conexões sem fio abrangem áreas de grande dimensão, interligando as diversas faculdades que cobrem um *campus* universitário, conferindo, assim, algumas vantagens como a diminuição de custos de acesso à Internet, e de mobilidade dos utilizadores. Na figura em baixo, pode-se constatar um mapa de uma rede Local sem Fios que cobre um *campus* universitário.

Ilustração 1 - Mapa de uma Rede sem Fio num Campus Universitário



Fonte - http://volnet.utk.edu/wireless/wirelessmap.html,

consultado a 10 de Julho de 2006

Estas infra-estruturas de redes sem fios num campo universitário, podem atingir conexões a altas velocidades, possibilitando a cobertura das faculdades, e proporcionando à comunidade de docente, dos funcionários e de alunos o acesso à rede, desde que disponham de um computador com placa de rede sem fios. Efectivamente, uma das grandes vantagens desta rede dentro de uma infra-estrutura de rede universitária é o facto das suas comunidades poderem aceder a rede através dos seus computadores pessoais, deste que estejam dentro da área coberta pelas Antenas que cobrem o *campus* e que tenham o computador configurado para obterem endereço, independentemente da plataforma que utilizam, possibilitando assim uma maior mobilidade dos utilizados da rede.

2.2.1.3 Virtual LANs

Uma VLAN é um agrupamento lógico de estações ou dispositivos de rede que podem ser reunidas por funções operacionais ou por departamentos, independentemente do local físico dos utilizadores. Este ajuntamento lógico de estações, serviços e dispositivos de rede não se restringe a um segmento físico de uma rede local. Assim pode-se dizer que VLAN é um agrupamento lógico de utilizadores independentemente das suas localizações físicas[6].

[6] cisco.netacad.net

Os dispositivos em uma VLAN só comunicam com os dispositivos existentes na mesma VLAN. Os roteadores providenciam a conectividade entre VLANs diferentes.

Existem 3 tipos de VLANs:

- Baseada em Porta que permite associar uma porta a um utilizador e uma porta a um seguimento. Este tipo de VLAN confere a máxima segurança ente VLANs e facilita o controlo da rede, embora exija um controlo mais exigente por parte do administrador.

- Baseada em endereços MAC que permite associar os endereços físicos de um computador a uma VLAN, permitindo assim maior mobilidade dos computadores, principalmente os portáteis.

- E finalmente, baseada em Protocolo utilizado pelas máquinas para associá-las a uma determinada VLAN.

Oferecem as seguintes vantagens:

- Aumentam o desempenho geral da rede pela agregação lógica dos utilizadores e recursos. Normalmente, as empresas utilizam VLANs como uma forma de assegurar que um dado conjunto de utilizadores esteja agrupado logicamente independentemente da sua localização física.

- Facilitam a administração de grupos lógicos de estações e servidores de modo que possam comunicar como se estivessem no mesmo segmento físico de uma rede local. Também facultam a administração de mudanças, acréscimos e modificações nos membros desses grupos.

- Segmentam logicamente as redes comutadas com base nas funções profissionais, departamentais ou de equipas de projectos, independentemente da localização física dos utilizadores ou das conexões físicas da rede. Todos os postos de trabalho e servidores utilizados por um grupo de trabalho em particular compartilham a mesma VLAN, independentemente da sua conexão ou localização física.

- Permitem que os administradores de redes organizem redes locais logicamente em vez de fisicamente. Esta é uma vantagem importante, porque permite que os administradores de redes realizem várias tarefas como, por exemplo, mover facilmente as estações de trabalho na rede local; adicionar postos de trabalho à rede local; modificar facilmente a configuração da rede local; controlar facilmente o tráfego da rede; e aumentar a segurança da rede.

A sua utilização nas universidades prende-se com o facto de facilitar a gestão dinâmica de mobilidades, tendo em conta que esta tecnologia permite a mobilidade dos utilizadores principalmente os que dispõem de computadores portáteis, possibilitando assim o acesso à rede de qualquer ponto onde existe a conexão à rede. Um outro aspecto é que ela facilita a gestão de tráfico, o que para as Universidade é vantajoso devido ao elevado número de utilizadores que dispõem, além de garantir alta segurança a nível lógico na gestão dos utilizadores.

2.2.1.4 Virtual Private Network

Uma **Rede Privada Virtual** (**Virtual Private Network - VPN**) é uma rede de comunicações privada normalmente utilizada por uma empresa ou um conjunto de empresas e/ou instituições, construída em cima de uma rede de comunicações pública (como por exemplo, a Internet).

Surgiu para superar problemas de segurança da informação, tendo em conta que funciona numa rede pública, é implementada através de protocolos de tunelamento e também por procedimentos de encriptação, integridade e autenticação. A sua utilização permite o acesso remoto por parte de profissionais que viajam frequentemente ou que precisam trabalhar em casa, acessando a rede interna da empresa para executar as suas tarefas.

Existem três tipos de VPNs:

- Access VPNs, que permite o acesso remoto para funcionários móveis e para pequenos escritórios/escritórios domiciliares (SOHO) à Intranet ou Extranet da matriz através de uma infra-estrutura compartilhada.

- Intranet VPNs que interliga os escritórios regionais e remotos à rede interna da matriz através de uma infra-estrutura compartilhada com a utilização de conexões dedicadas. Estas diferem das Extranet VPNs dado que só permitem o acesso aos funcionários da empresa.

- E finalmente as Extranet VPNs que ligam os associados empresariais à rede da matriz através de uma infra-estrutura compartilhada com a utilização de conexões dedicadas. Extranet VPNs diferem das Intranet VPNs dado que só permitem o acesso aos usuários externos à empresa.

Tendo em consideração os avanços tecnológicos, sobretudo o acesso à Internet que actualmente é cada vez mais acessível para todos, as universidades utilizam a tecnologia de Rede Privava Virtual para facilitar a toda a comunidade académica o acesso aos recursos da rede sem estarem fisicamente na universidade. Sendo que as universidades dispõem de numerosos utilizadores, e dado que existem alunos de diversos cursos leccionados em cada faculdade, a tecnologia VPN facilita não só o acesso a recursos remotamente mas também à própria racionalização de recursos de *hardware* e espaços físicos.

A utilização de VPN carece também de alguns cuidados de segurança, como, por exemplo, a utilização de autenticação, baseada em senhas de alta segurança para impedir ataques.

2.2.1.5Gestão das Redes Universitárias

As redes universitárias devem actuar sempre na prevenção, investigação e respostas a incidentes de segurança, de forma célere de modo a garantir uma segurança cada vez mais rígida. A gestão das redes Universitárias deve partir da estrutura orgânica do departamento de informática. Este deve ser bem organizado de modo que todas as estruturas funcionem devidamente. Não se pode ter um departamento onde todos os serviços necessários são centralizados, deve existir, sim, departamentos que retractam aspectos de Manutenção e Suporte, Redes e Desenvolvimento.

No departamento de Manutenção e Suporte, é imperativo o funcionamento activo dos serviços de HelpDesk para que quando os utilizadores precisem dos seus serviços possam ser atendidos rapidamente de modo a gerar maior produção do pessoal colaborador. Na divisão de Redes, devem existir os serviços de administração de sistemas, como a configuração e manutenção de servidores e serviços de conectividade. E finalmente, o sector de desenvolvimento, que é uma componente importante para a criação de novos recursos e ferramentas, necessita de condições necessárias para desenvolver projectos.

A gestão da rede universitária deve centralizar num conjunto de elementos que são cruciais para o funcionamento da rede nomeadamente:

- O administrador deve conhecer muito bem a estrutura da sua rede física e lógica.
- Deve-se investigar de incidentes, actuando na prevenção contra ataques internos e externos, Spam e Virus.
- Deve-se ter capacidades de dar respostas a incidentes nomeadamente através de identificação e punição de ataques internos, mas para isso devem existir políticas internas que definem visivelmente as políticas de segurança organizacional e os incidentes externos através de mecanismos de identificação da rede e/ou do computador remoto e adopção de medidas restritivas de acesso através do firewall.
- Deve-se ter sistemas de detecção de intrusão activos e funcionais, firewall funcional, sistemas operativos com versões actualizadas, políticas de segurança local implementadas nos servidores e documentação de actividades para uma resolução mais rápida de problemas comuns.

A gestão da rede passa por um conjuntos de medidas:

- Uma boa política de distribuição de recursos como por exemplo os recursos de *hardware* como computadores e impressoras e de *softwares* como ferramentas de trabalho e informações de acesso.
- Gestão e configuração de servidores de acesso como, por exemplo, servidores de correio electrónico, de programas e de autenticação, de modo a facilitar um acesso seguro à rede e aos serviços da rede, garantindo sempre as normas de segurança.

- Gestão da largura de banda de modo que a rede não fique lenta e a adopção de políticas que impeçam a utilização de programas ou serviços que despendem muita largura, principalmente nos horários de trabalho.
- Serviços de Helpdesk funcional e rápido em casos de pedidos de solicitação, de modo que os recursos da rede estejam sempre disponíveis e utilizáveis.
- Gestão dos equipamentos de rede, de forma a garantir a conectividades dos postos de trabalho e das impressoras de rede.
- Backups centralizados, garantindo a salvaguarda da informação, tendo em conta que este é o bem mais precioso de uma universidade.

2.2.2 Gestão Académica e Tecnologias de Ensino

2.2.2.1 Portal Universitário

Enquanto que um Sítio Web tem uma colecção de aplicações, um Portal tem uma única porta de entrada a várias aplicações, que dão acesso a diversas informações (Rosa, 2005).

Um portal de Web pode ser definido como um local de Web para uma utilização específica, que agrega uma ordem de conteúdos e provê uma variedade de serviços, inclusive a procura de máquinas, directórios, notícias, e-mail e etc, (Pienaar, 2003).

Segundo este autor, existem vários tipos de portais:

- **Portal Vertical**, desenvolvidos para grupos de interesses específicos, por exemplo CNET.com (centro comercial) e women.com (Assuntos de mulheres).
- **Portal Horizontal**, desenvolvidos para uso geral, por exemplo: Yahoo, AltaVista e AOL.com.
- **Portal de Empreendimento**, destinados a vendedores, permitem a integração de informação de múltiplas bases de dados e formatos de ficheiros.
- **Portais de busca**, destinados para pesquisas, por exemplo motor de busca ou bibliotecas digitais.

Segundo (Rosa, 2005), para que se possa garantir acesso aos recursos disponibilizados numa Universidade digital, através de um único ponto de acesso incluindo um mecanismo centralizado de autenticação de forma a garantir a disponibilidade dos recursos em tempo real, é necessário construir um Portal Universitário.

Nos meios académicos, pode-se conseguir uma prestação de serviço personalizado, através de uma interface Web, que pode apoiar o desempenho das tarefas (ensino e pesquisa). Para a concepção do portal adequado a meios académicos (Pienaar, 2003), defende que deve ser colocado um conjunto de questões:

- O que pode ser visto como sendo a administração pessoal de conhecimento académico e da informação? Qual é o impacto da Internet no ciclo de conhecimento científico?

- Até que ponto o conceito e funcionalidade de Web portais apoiam a administração pessoal de conhecimento e da informação de académicos?

- Que fontes de informação, serviços e ferramentas devem fazer parte de tal portal?

- Como é aceitado a ideia do portal Web, pelos académicos e que problemas eles se antecipam quanto à implementação do portal?

- Os itens considerados no desenho do portal são suficientes? O portal pode ter sucesso com o desenvolvimento e implementação destes itens?

Este autor defende que o ciclo de conhecimento científico consiste nos seguintes sectores:

- **Sector de utilizador** – pesquisa de literatura, assimilação e formulação de hipóteses;
- **Sector de Generação –** teste experimental e desenvolvimento de nova teoria;
- **Sector de comunicação –** relatórios orais em reuniões, documentos escritos, publicação primária, secundária e ternária;
- **Sector de armazenamento** – aquisição e processando para recuperação, o armazenamento do conhecimento em bibliotecas, arquivos etc;

Após identificar as fases do conhecimento científico Heila Pienaar (2003), questiona qual seria uma possível influência da Internet e do portal no ciclo de conhecimento científico, da seguinte forma:

- **Sector de Utilizador:** as máquinas sofisticadas são bem direccionadas para os utilizadores finais? As bases de dados tradicionais são projectadas para funcionar em ambientes de *web*?

- **Sector de Generação:** os produtos de conhecimento podem ser criados por Editores de Web e publicadas na *Web*?

- **Sector de Comunicação:** os instrumentos de comunicação da Internet, anúncios, listas de servidores, de *e-mail* suportam facilidades de apoio internacional e a criação de comunidades virtuais? Publicações tradicionais (diários, livros, dissertações) são publicadas na Web? Material de educação é entregue pela Web (*e-education*)?

- **Sector de armazenamento:** as informações e conhecimentos científicos são electronicamente armazenados e disponíveis na Web? Bibliotecas digitais são desenvolvidas para administrar a informação científica na Web?

Por conseguinte, este autor defende que um portal académico deve respeitar todos os itens enumerados no parágrafo anterior.

A JA-SIG[7] especifica como é que deverão ser os portais universitários, definindo um conjunto de características que deverão possuir:

- Fornecer acesso a todas as informações e serviços através de uma única interface gráfica e possibilitar um ponto único onde todas as transações poderão ser realizadas.
- Suportar autenticação única para acesso aos recursos e aplicações.
- Possibilitar a apresentação de informações e acesso aos serviços de forma individualizada e personalizada.

[7] http//www.ja-sig.org

- Permitir a cada membro da comunidade universitária efectuar a personalização do seu ambiente de trabalho no portal
- Garantir à Universidade o controlo total e a gestão dos conteúdos e da Interface.
- Ser independente do vendedor, isto é, não ser preso a *hardware* e/ou *software* proprietários.
- Estar disponível 24 horas por dia e 7 dias por semana a todos os utilizadores.
- Ser flexível e susceptível de integrar novas tecnologias e novas aplicações.

2.2.2.2 Sistemas de Informação Académico

A Universidade, enquanto organização com necessidades e desafios em termos do processamento de informação, não deverá relegar para planos secundários o estudo, a concepção e implementação de sistema que se destina à gestão do Processo de Ensino-Aprendizagem, Silva (2006).

Assiste-se, nos últimos anos, a um cenário cada vez mais familiar de avanços tecnológicos nas áreas de informática e comunicação. Esses avanços ficam mais visíveis através das redes de computadores, das quais a Internet, é certamente a mais conhecida. Segundo (Imre,1997), uma reflexão mais cuidadosa revela que no centro desta revolução tecnológica encontra-se **o conceito da informação**. Informação, intimamente ligada a conhecimento, não possui uma definição precisa, embora Imre acredite que ela esteja suficientemente bem caracterizada para não deixar dúvidas a que se refere. Pois bem, os avanços tecnológicos se reflectem em mudanças marcantes que influenciam a geração, a transformação, o armazenamento, a transmissão e a recuperação da informação.

Na perspectiva de (Silva, 2006)[8], o fluxo de informação dentro de uma organização está definido nos seus vários processos do trabalho. Para gerir com eficácia essas informações são

[8] Actas da 1ª Conferência Ibérica de Sistemas e Tecnologias de Informação, Modelos Organizacionais e Sistemas de Informação

necessários os meios humanos e tecnológicos que auxiliam e impulsionam a sua optimização, originando, assim, sistemas de informação.

Se aceitarmos que a revolução tecnológica vai afectar tudo que está ligado ao conceito da informação, é forçoso concluir que as próprias universidades serão profundamente afectadas pelo processo, (Imre, 1997). Este autor defende que um outro motivo determinante pelo qual as universidades são e serão profundamente afectadas pelo fenómeno em questão é o fato da informação ser o sumo mais importante e mais palpável em torno do qual se situa o próprio conceito da universidade.

O **sistema de informação** segundo Silva (2006) apud Laudon & Laudon (2005), é um conjunto de componentes interrelacionados que recolhe ou retira, processa, armazena e distribui informação para suportar tomadas de decisão, coordenar e controlar processos de trabalho. Este autor salienta que as tecnologias de informação por si só não permitem a uma organização gerir adequadamente a informação, porque esta tem que estar adequada às necessidades do sistema de informação e em consonância com os objectivos e as estratégias da organização.

No que concerne aos sistemas de informação nas universidades, para o suporte ao ensino-aprendizagem, (Silva, 2006), defende que este deve contribuir para a participação de forma activa e inovadora no desenvolvimento humano, integral e ecológico dos diferentes grupos etários e sociais. Segundo este autor, necessita de meios para a promoção da eficácia na gestão do processo de ensino, realização de investigação enriquecidora, promoção do conhecimento indógino e criação de uma forma de trabalho bem qualificada.

Para a sua materialização, as exigências da sua concepção vai na mesma linha das preocupações com a informação de uma organização, que é implementar soluções em que a universidade, enquanto organização procura formas de eficácia nos seus processos e na implementação de sistemas de informação cujo o núcleo é baseado na recolha, armazenamento e disseminação de informação com interesse directo ou indirecto no processo de ensino-aprendizagem.

Um sistema de informação que apoia a administração de conhecimento pessoal de académicos deve ter os seguintes requisitos, na perspectiva de Pienaar (2001):

- Administração de conhecimento pessoal: o académico deve ser capaz administrar toda sua informação e conhecimento de uma maneira integrada com a ajuda de um ambiente electrónico.

- Colecção e recuperação de informação: a informação do sistema tem que apoiar o académico na procura de informação electrónica.

- Organizando Pessoal e processando de informação: a informação do sistema tem que promover uma variedade de fontes de informação, por exemplo, literatura, informação organizacional interna e pessoal informação.

- Comunicação e distribuição do conhecimento: a criação e distribuição de conhecimento, como, por exemplo, artigos, relatórios e conferências, devem ser apoiados pela Comunicação Académica que, por sua vez, deve ser sustentado pelo Sistema.

A universidade, assim como outras organizações, enfrenta desafios de ambientes externo e interno. Em relação ao primeiro, numa sociedade de informação em que se vive actualmente onde os saberes se diversificam, a universidade deve dispor de ferramentas que permitam uma docência e investigação cada vez mais rica e capaz de acompanhar as mudanças do mundo exterior. Em relação ao ambiente interno, caracteriza-se por uma heterogeneidade de serviços, tecnologias e utilizadores com funções diferenciadas, que surge da necessidade de implementar soluções que permitam à universidade ter um total controlo do fluxo das informações e a tomada de melhores decisões.

Num sistema de informação académico, na perspectiva de Paulo Silva (2006) existem processos de suporte à gestão organizacional, de suporte ao processo ensino-apredizagem, de apoio à decisão a nível dos órgão do governo da instituição, o que aumenta o grau de complexidade de um sistema de informação, que responda de forma adequada a todos os requisitos exigidos por todos esses processos.

Segundo este autor, um Sistema de Informação Académico deve ter os seguintes Objectivos:

- Criar um repositório de informação que representa digitalmente toda a informação relacionada com o funcionamento dos cursos da Universidade.
- Fornecer ferramentas que permitem a exploração e navegação no espaço de informação académica: alunos, docentes, funcionários, cursos, disciplinas, áreas científicas, departamentos, projectos de investigação e publicações.
- Melhorar a comunicação dentro da Universidade.
- Permitir a interacção com sistemas das unidades de serviços financeiros, de documentação e Plataforma de *E-leaning*.

A necessidade de um sistema de informação académico nas universidades prende-se com o facto, desta instituição ser complexa devido à heterogeneidade dos diversos utilizadores inseridas dentro do contexto organizacional universitária. Esta complexidade exige uma forma de determinar um modelo de como as informações são representadas digitalmente e apresentadas através do Sistema de Informação Académico.

Dentro daquilo que é definido como informação académico existem entidades produtoras da informação e utilizadores da informação que naturalmente exigem um perfil de acesso diferente. No que concerne à estrutura arquitectónica de um sistema de informação académico, este autor defende a existência de pelos três componentes:

- Uma base de dados da informação
- Um nível acima de base de dados que contém toda a lógica computacional para a manipulação dos dados
- Uma interface que define a interacção entre os utilizadores e os módulos aplicacionais implementados.

2.2.2.3 Biblioteca Digital

Segundo (Noerr, 2003), existem duas alternativas convencionais para o conceito de Bibliotecas Digitais: “Bibliotecas que contém materiais de forma digitalizada” e “Biblioteca que contém material Digital”. As que contém material digital, é considerado que nasceram digital como por exemplo um texto criado em um processador de texto. As de forma digitalizada, pode ser considerada aqueles que foram transformadas em digital, convertendo documentos em formato digital conservando assim, as limitações para o seu manuseio.

Uma **Biblioteca Digital** permite o acesso remoto através de um computador com ligação em rede e/ou Internet, ao mesmo tempo, a sua utilização simultânea por diversos utilizadores, onde estes podem encontrar em suporte digital os produtos e serviços característicos de uma biblioteca física. Através dela é também possível utilizar de forma integrada diferentes suportes de registo de informação (texto, som, imagem), eliminado assim as barreiras físicas e a distância, factores que desde sempre limitaram o âmbito das bibliotecas físicas.

As bibliotecas são, por si, um contributo importante para facilitar a gestão da informação. Falando de bibliotecas Digitais Universitária dentro do contexto de Redes Universitárias e os seus recursos segundo Mariângela Fijita ([S/D]), é um sistema de informação que é parte de um sistema mais amplo, que poderia ser chamado sistema de informação académico, no qual, a geração de conhecimentos é o objecto da vida universitária. Também por outro lado, integra-se a sistemas de informação locais, regionais, nacionais e internacionais, considerando-se sua função social de divulgação do conhecimento.

Dentro daquilo que constitui a essência da Universidade, bibliotecas digitais e o seu acesso é muito importante tendo em conta que permite a colecção dos novos formatos documentários, acelera o processo de socialização do conhecimento da Universidade e amplia o conjunto de utentes da biblioteca universitária que, tradicionalmente, atingia somente o usuário local e agora atinge usuários virtuais.

A biblioteca digital, dessa forma, é importante no contexto da Universidade porque pode ser constantemente construída a partir do conhecimento gerado por suas pesquisas em formato documentário que propicia a divulgação do conhecimento a um amplo leque de usuários externos que, de modo tradicional, a biblioteca não teria como atingir. Nesse sentido, a

biblioteca universitária está modificando e reforçando cada vez mais sua infra-estrutura física, material e de recursos humanos para a implantação e manutenção da biblioteca digital, favorecendo a existência de uma dinâmica de intenso relacionamento social e alto grau de inter-conectividade institucional para troca de conhecimento.

2.2.2.4 Ensino à Distância

Ensino a distância segundo (Aretio,1994) apud (Rurato et all [S/D]), é um sistema tecnológico de comunicação bidireccional que pode ser massivo e que substitui a interacção pessoal na sala de aula entre o professor e o aluno, como meio preferencial de ensino, pela acção sistemática e conjunta de diversos recursos didácticos e pelo apoio de uma organização e tutoria que proporcionam a aprendizagem independente e flexível dos alunos.

(Mehlechke et Tarouco, [S/D]), apresenta quatro componentes necessárias para o sistema de educação a distância:

- O **aluno** como sendo o centro do processo educativo.
- O **docente** que será o motivador e promotor da aprendizagem cooperativa e interactiva no ambiente virtual.
- A **comunicação** que poderá ser realizada através de material impresso, audiovisual, telemática (Internet, *softwares*, CD-ROM, vídeo interactivo, hipermídia, entre outros) e a tutoria mediando o presencial e o virtual.
- A **estrutura e organização** dos materiais, a distribuição de materiais, o processos de comunicação e a avaliação que fazem parte do processo inicial no desenvolvimento de programas de ensino a distância.

Existem 6 categorias de **características do ensino a distância**: (Rurato et all [S/D]).

1. **A base de estudo a distância é um curso pré-produzido**, este deve ser auto-instrutivo, acessível ao estudo individual sem necessidade do professor em situações de registo áudio, vídeo, programas da rádio e televisão, via videoconferência ou Internet.

2. **Comunicação organização em duas direcções (Bidireccional)** – existem um lugar entre os alunos e/ou entre alunos e uma organização de apoio.
3. **Estudo individual** – destina ao aluno isolado, no estudo que se realiza por si próprio
4. **Forma massiva de Comunicação**, uma vez que existe um número elevado de aluno
5. **Inclui método de planeamento e procedimentos de realização** destacando (divisão de trabalho, mecanização, automatização, controlo e verificação).
6. **Estudo a distância**, está organizada e mediatizada de conversação e didáctica guiada.

Peters (2001) apud (Mehlechke et Tarouco, [S/D]), apresenta um conjunto de modelos relacionados ao ensino a Distância:

- **Ensino por correspondência**: material impresso (livros didácticos).
- **Ensino a distância clássico**: material diversificado como material impresso, televisão, rádio, audiovisuais, tutores.
- **Ensino a distância com base na pesquisa**: caracterizado pela leitura de cursos de ensino a distância impressos e na frequência parcialmente obrigatória em seminários. Concede apenas o grau superior ou de mestre.
- **Ensino a distância Grupal**: programações didácticas, mediante a rádio e televisão, associadas a actividades regulares obrigatórias, com presença.
- **Ensino a distância autónomo**: planear, organizar e implementar isoladamente. A universidade apenas aconselha, incentiva, assiste e fornece certificado.

A característica fundamental da actual crise do ensino superior é a sua incapacidade de enfrentar os desafios e dar respostas adequadas às necessidades sociais de um mundo globalizado que não é solidário na produção, distribuição e utilização democrática do conhecimento. Os países que têm um claro projecto de nação, com objectivos e metas bem definidos, conseguem soluções mais consistentes no campo educacional, mais ou menos democráticas, de acordo com modelos socialmente mais includentes ou excludentes que adotem. Existe consenso de que investimentos em educação, ciência e tecnologia são necessários para assegurar soberania nacional, para o que é imprescindível o ensino superior. Neste contexto o Ensino a Distancia é fundamental para as Universidade do século XXI[9].

[9] Seminário Internacional da Universidade do Século XXI, http://portal.mec.gov.br/sesu/arquivos/pdf/novoscaminhoseducacaosuperior.pdf#search=%22ensino%20a%20dist%C3%A2ncia%20%2B%20universidades%20%5Bpdf%5D%22

Capitulo 3 : A Segurança Informática

3.1 Aspectos Históricos

Desde o início da civilização humana houve uma preocupação com as informações e com os conhecimentos atrelados a elas. Antigamente, isso foi observado no processo de escrita de alguns povos, como é o caso da antiga civilização egípcia, na qual somente as castas "superiores" da sociedade tinham acesso aos manuscritos da época. Assim a escrita, por meio de hierogrifos do Egipto antigo, representava uma das várias formas utilizadas pelos antigos de protegerem e, ao mesmo tempo de perpetuarem o conhecimento, (Long, [S/D]).

Na sociedade moderna, com o advento do surgimento dos primeiros computadores, houve uma maior atenção para a questão da segurança das informações. Inicialmente esta preocupação era muito rudimentar, porém, com o passar do tempo este processo mudou e agora a segurança da informação é considerada a arma de sucesso para as organizações.

Levando em consideração que as tecnologias de redes de dados e sistemas de informação impulsionam o aparecimento de ambientes heterogéneos nas organizações e tendo em conta que à medida que evoluem as tecnologias, aumenta a necessidade de acompanhar essa evolução tecnológica, a questão da segurança tornou fundamental para a sobrevivência das organizações.

Segundo , (Long, S.D), a questão da segurança no âmbito dos computadores ganhou força com o surgimento das máquinas de tempo compartilhado (time-sharing), permitindo que vários utilizadores pudessem ter acesso às mesmas informações.

Em outubro de 1967, nasceu nos Estados Unidos o primeiro esforço para solucionar tal situação, com a criação de uma "força tarefa", que resultou em um documento entitulado **“Security Control for Computer System”**, que representou o início do processo oficial de segurança, com a criação de um conjunto de regras para segurança de computadores que mais tarde, deu origem a publicação da uma Norma Internacional de Segurança da Informação no ano de 2000.

Seguidamente, em outubro de 1972, foi escrito um relatório técnico denominado: "*Computer Security Technologs Planning Study*", no qual foi descrito os problemas envolvidos no processo de se fornecer os mecanismos necessários para salvaguardar a segurança de computadores.

Em 1977, o Departamento de Defesa dos Estados Unidos formulou um plano sistemático para tratar do Problema Clássico de Segurança, o qual deu origem ao "DoD - Computer Security Initiative", que por sua vez deu origem a um "**Centro**", criado para avaliar o quão seguro eram as soluções disponibilizadas. Esta iniciativa, gerou a necessidade da criação de um conjunto de regras que ficou conhecido informalmente como "*The Orange Book*". Este permitiu a produção de uma larga quantidade de documentos técnicos, que representaram o primeiro passo na formação de uma norma coesa e completa sobre a segurança de computadores.

O "*The Orange Book*", hoje considerado ultrapassado mas, representou um marco "zero", do qual nasceram vários padrões de segurança, cada qual com a sua filosofia e métodos proprietários, visando uma padronização mundial.

Depois desta fase, houve um esforço para a construção de uma nova norma, mais actual e que não se detivesse somente na questão da segurança de computadores, mas sim na segurança de toda e qualquer forma de informação.

Este esforço foi liderado pela "*International Organization for Standardization (ISO)*. No final do ano de 2000, o primeiro resultado desse esforço foi apresentado, que é a norma internacional de Segurança da Informação "ISO/IEC-17799:2000", a qual já possui uma versão aplicada aos países de língua portuguesa, denominada "NBR ISO/IEC-17799".

A ISO (*International Organization for Standardization*), por sua vez define segurança como a tentativa de minimizar a vulnerabilidade de valores e recursos, (Carneiro, 2002).

3.2 Conceito da Segurança

A segurança é um mecanismo de controlar e evitar as chamadas vulnerabilidades que é, qualquer tentativa de penetrar num SI sem qualquer autorização no sentido de tirar proveito do seu conteúdo ou das suas características nomeadamente a configuração e alcance…"(Carneiro, 2002).

A segurança, segundo este Autor, tem como finalidade preservar os activos e os recursos físicos e humanos contra roubo, incêndio, inundações e até contra factores de ordem sociais, como greves, atentados que podem comprometer a existência e o funcionamento da própria organização. No domínio da Informática a segurança dos sistemas refere-se tanto aos conceitos de segurança física como da lógica.

Na segurança física refere-se a aspectos como a protecção de *Hardware*, dos equipamentos periféricos e instalações onde se encontram montados e a prevenção contra situações de incêndios, sabotagens, roubos, inundações e acentuadas alterações térmicas e catástrofes naturais.A segurança lógica refere-se a protecção de dados contra acessos não autorizados ou suportes lógicos maliciosos.

Segundo (Carneiro, 2002), a segurança dos sistemas de informação é um conjunto de medidas e procedimentos, que têm por finalidade evitar que a informação seja destruída, alterada, ou acedida acidentalmente ou intencionalmente de forma não autorizada.

Para isso há que implementar mecanismos que impeçam qualquer tipo de instabilidade no funcionamento dos sistemas, começando desde a segurança física, passando para a segurança da informação disponibilizada, para a segurança das pessoas que utilizam estas informações até à segurança lógica do próprio sistema.

3.3 Tipos da Segurança Informática

3.3.1 Segurança da Informação

Cada vez mais os gestores de topo e responsáveis pelos **SI** informatizados das empresas se preocupam com a Segurança dos Sistemas e com as consequências que um incidente pode trazer para o funcionamento dos seus **SI**, no que tange à confidencialidade, integridade e disponibilidade da informação. O **SI** informatizado contém dados e informações de natureza confidencial e que por isso, necessitam de uma protecção particular, para que não sejam utilizadas por pessoas não devidamente autorizadas ou divulgadas a entidades perante as quais a empresa pretenda defender a sua privacidade.

Na perspectiva de (Silva, Carvalho et al, 2003), a vantagem competitiva duma organização, assenta muitas vezes na informação que detêm e na capacidade de controlar a sua divulgação. Por exemplo, para as organizações de investigação e desenvolvimento esta propriedade é fundamental. Neste contexto, a existência de mecanismos que garantam a confidencialidade das informações, mas que não impeçam o seu acesso atempado às pessoas autorizadas é importantíssimo.

O valor da informação, segundo este autor está na sua fiabilidade, por isso a integridade da informação é um dos aspectos vitais relativamente aos dados armazenados, processados e transmitidos pelos Sistemas de Informações. A existência de mecanismos de validação da informação é extremamente importante, a integridade é igualmente importante para a recuperação da informação perdida, uma vez que o valor das cópias que não apresentam a integridade é praticamente nula. Nesta óptica, as medidas de protecção dos dados deverão contemplar aspectos que facultem o acesso aos mesmos, porém, deverão ser capazes de fazer a distinção entre acessos autorizados e não autorizados.

O acesso atempado à informação, é vital e dele depende a prossecução dos objectivos da empresa, porque possuir a informação necessária mas não tê-la disponível no tempo atempado é o mesmo de não possuir qualquer tipo de informação. Para isso há que implementar a segurança físicas e lógicas de modo a garantir a segurança da informação.

3.3.2 Segurança Física

A Segurança física consiste na aplicação de barreiras físicas e procedimentos de controlo, como medidas de prevenção e contra medidas perante ameaças aos recursos e informação confidencial. Refere-se aos procedimentos de controlo e aos mecanismos de segurança dentro e em volta do Centro de Processamento de Dados, assim como os meios de acesso remoto implementados para proteger o hardware e os meios de armazenamento de dados, (Silva, Carvalho et al, 2003).

O principal objectivo da segurança física é garantir a protecção dos **SIs** quanto às suas dimensões físicas e no que se refere a todos os seus componentes, nomeadamente *hardware*, *software*, documentação e meios magnéticos. Esta protecção relaciona-se com riscos por divulgação, perda, extravios ou por danos físicos. Pode-se ter segurança física a três níveis: Segurança do pessoal, das instalações e dos equipamentos.

A segurança do pessoal tem como objectivo, reduzir os riscos devido a erros humanos, roubo, fraudes e/ou má utilização dos recursos existentes. A do equipamento tem por objectivo, proteger o *hardware* computacional e outros equipamentos, as suas interligações e o fornecimento de energia. Por último a segurança das instalações, que trata dos requisitos de localização e a estrutura dos edifícios destinados aos centros de informática de forma a garantir um nível de segurança adequado.

3.3.2.1 Segurança do Pessoal

A segurança do pessoal é um aspecto muito importante dado que são as pessoas que interagem diariamente com os sistemas, que tem acesso às informações contidas no sistema,

por isso, muitas vezes são as principais ameaças a esses sistemas. (Silva, Carvalho et al, 2003), defendem que deve-se ter muito cuidado no recrutamento de pessoas, porque estas podem ser possíveis perigos à segurança nas organizações. Dentro da Segurança do Pessoal pode destacar:

- **Segurança nos Conteúdos Funcionais e no Recrutamento**

- **Formação dos Utilizadores**

- **Resposta a Incidentes**

A Segurança nos Conteúdos Funcionais e no Recrutamento, tem como objectivo reduzir os riscos de erros humanos na utilização do sistema, roubo, bem como a má utilização dos recursos das tecnologias de informação e comunicação disponibilizados. No que tange à segurança nos conteúdos funcionais e de recrutamento, estes defendem a segurança desde o recrutamento até à postura que os utilizadores devem ter na utilização do sistema.

Na Formação dos Utilizadores, defendem que os utilizadores devem receber formação em segurança e numa correcta utilização das **TI** (Tecnologias de Informação) para um normal funcionamento dos sistemas e da política de segurança implementada. A sensibilização dos utilizadores garante que estes tenham mais consciência das ameaças e preocupações respeitantes à segurança da informação e estejam mais dispostos em apoiar na implementação do programa da política de segurança organizacional.

E finalmente a Resposta a Incidentes**,** Segundo (Silva, Carvalho et al, 2003), um incidente de segurança é qualquer acontecimento que pode originar perda ou dano dos recursos da organização, ou uma acção que afecte os procedimentos de segurança na organização.

Este autor defende que o conhecimento desses incidentes por parte dos utilizadores do sistema é fundamente para minimizar as consequências que advém destes incidentes, por isso, é muito importante que estes saibam a forma mais fácil e rápida para comunicar estes incidentes. Neste caso a formação de utilizadores neste aspecto é fundamental para solucionar problemas, quando acontecer qualquer incidente.

3.3.2.2 Segurança das Instalações

A localização e a estrutura das instalações de um centro de informática deve respeitar um conjunto de requisitos físicos e ambientais, que permita garantir a sua segurança. Existem normas estipuladas internacionalmente para a localização de uma instalação informática, estes devem ficar em lugares adequados para ir em consonância com a própria palavra segurança. Dentro da segurança das instalações pode-se falar da Localização e Estrutura dos Centros de Informática e Áreas de Segurança.

Segundo (Ferreira, 1995), a localização das instalações de um centro de informática não deve ficar nem no edifício térreo nem no último piso do edifício, no caso do edifício térreo, o centro deve ficar localizado na zona mais resguardada possível, longe das vias de circulação pública (…). Antes de se fazer um projecto de rede, deve-se levar em consideração o lugar mais adequado para fazer um centro de informática, muitos autores aconselham que sejam lugares com controlo de acesso físico como cartões magnéticos ou sistemas biométricos, afastados das vias de circulação pública e canos de água.

Em relação às Áreas de Segurança**,** estas, são lugares onde existem recursos das TI sensíveis ao funcionamento da organização senão a sua própria sobrevivência, porque acessos não autorizados a essas áreas e aos sistemas podem originar consequências catastróficas à organização. Os recursos das TI que suportam actividades críticas ou sensíveis como os servidores devem estar instalados em áreas de segurança, segundo (Ferreira, 1995).

3.3.2.3 Segurança do Equipamento

A segurança do equipamento, é um outro ponto da segurança física que impede a perda, dano e acesso não autorizados aos equipamentos duma organização, implementando medidas de segurança desde a sua instalação, manutenção até a sua destruição.

A segurança do equipamento, deve impedir acessos não autorizados mas, nunca deve por em causa a disponibilidade e a integridade do mesmo. Isto porque a concepção de mecanismos de segurança não pode pôr em causa o acesso dos utilizados, nem a validade da informação.

3.3.3 Segurança Lógica

A informação em suporte digital encontra-se exposta a ataques. Alguns destes ataques são passivos, na medida em que apenas capturam os dados, sem os alterar, enquanto que outros são activos, afectando a informação com o intuito de a corromper ou destruir, (Silva, Carvalho et al, 2003).

Alberto carneiro in Introdução à Segurança dos Sistemas de Informação, diz que " *a segurança lógica baseia-se na gestão das autorizações de acesso aos recursos informáticos, na identificação e na autenticação, na medida em que a gestão abarca no processo de pedido, acompanhamento e encerramento das contas dos utilizadores, no processo de revisão periódica das* ***contas dos utilizadores e autorizações*** *estabelecidas"*.

Este autor defende que a segurança lógica deve restringir o acesso aos programas e arquivos, assegurando que os utilizadores trabalham sem supervisão e não modifiquem nem os programas nem os arquivos que não correspondem ao seu domínio de trabalho.

Mas para garantir a segurança lógica, é necessário garantir primeiramente a segurança da informação, através do perfil de utilizadores que acedam ao sistema, porque a razão de ser da segurança lógica é segurar a informação no formato digital. Mas afinal o que é a informação?

Segundo (Amaral & Varajão, 2000), a informação é aquele conjunto de dados que, quando fornecido de forma em tempo adequado, melhora o conhecimento da pessoa que o recebe, ficando ela mais habilitada a desenvolver determinada actividade ou a tomar determinada decisão. Este autor defende que a informação é tida actualmente como uma das armas de sucesso para as organizações como também um passo essencial na definição e implementação de medidas eficazes de salvaguarda bem como a existência de uma clara identificação dos proprietários da informação na organização.

A classificação da informação deverá ser orientado por definições claras dos diferentes graus de sensibilidade da informação, reconhecidos pela empresa, bem como pela determinação exacta dos responsáveis pela classificação, (Silva, Carvalho et al, 2003).

Silva acrescenta na mesma obra que, para que o processo da classificação da informação seja viável, é muito importante perceber quais as consequências da divulgação, alteração ou eliminação não autorizada dos dados classificados para a organização. Este esforço de nada servirá se não for seguido de medidas de protecção adequadas aos níveis de classificação atribuídos.

A classificação de informação segundo (Silva, Carvalho et al, 2003), permite desenvolver níveis de protecção idênticos para a informação com os mesmos requisitos de segurança e permite também definir padrões de protecção, claros e inequívocos, para as várias categorias de classificação. Para estes autores, toda a informação classificada de "**vital**" deverá ser objecto de controlo de acessos, autorizado superiormente pela administração.

(Ferreira, 1995), divide a segurança lógica em três pontos: A gestão do sistema informático e da rede, a segurança dos sistemas aplicacionais e a gestão e o controle de acesso.

3.3.3.1 Gestão do Sistema Informático e da Rede

A gestão do sistema informático é a base da segurança da rede de qualquer organização. Uma rede onde não há segurança nos sistemas informáticos, é uma rede muito vulnerável a ataques. Neste tipo de segurança existem um conjunto de pontos que devem ser seguidos para manter a segurança neste domínio, nomeadamente:

- Procedimentos e Responsabilidades de exploração
- Planeamento e aceitação do Sistema
- Protecção contra suporte lógico malicioso
- Gestão da Rede
- Tratamento e Segurança de Suportes informáticos

O Procedimentos e a Responsabilidades de exploração, tem por objectivo garantir a exploração segura e correcta dos recursos de processamento e de rede, estabelecendo responsabilidades e procedimentos na gestão e exploração dos recursos informáticos, disponibilizando documentos de utilização, bem como estabelecer responsabilidades de modo a minimizar incidentes e má utilização desses recursos.

O Planeamento e aceitação do Sistema, tem por objectivo, minimizar o risco de falhas dos sistemas informático. No planeamento e aceitação do Sistema, são exigidos previamente, o planeamento e a preparação dos recursos informáticos como: As capacidades de armazenamento como memórias internas e externas, o planeamento das utilizações actuais e tendências futuras dos recursos informáticos, a aquisição de novas tecnologias de modo a garantir a disponibilidade de recursos e capacidades adequados segundo as necessidades presentes e futuras.

Na Protecção contra suporte lógico malicioso, devem ser adoptadas medidas de protecção, detecção contra suporte lógico malicioso, bem como a consciencialização dos utilizadores, de forma a assegurar a protecção e a integridade do suporte lógico e de dados. O controle de vírus, por exemplo, deve ser efectuado em apropriados sistemas bem como a sua actualização. A organização deve estabelecer uma política formal, usando *softwares* licenciados e proibindo a utilização dos *softwares* piratas, (Ferreira, 1995).

A Gestão da Rede, permite garantir a segurança da informação em circulação na rede é o principal objectivo da gestão da rede. Para isso, uma atenção especial deve ser feita através duma série de controlos de segurança na rede, para garantir segurança dos dados transportados pela rede e protecção da conexão contra acessos não autorizados.

Relativamente ao Tratamento e Segurança de Suportes informáticos**,** este tem como objectivo principal impedir danos nos recursos informáticos e interrupções nas actividades do funcionamento do sistema. Os suportes informáticos, devem ser controlados e protegidos fisicamente, os removíveis devem ser controlados, os dados sensíveis devem ter procedimentos de tratamento e a documentação do sistema deve ser protegida contra acessos não autorizados,(Ferreira, 1995).

3.3.3.2 Segurança dos Sistemas Aplicacionais

A segurança dos sistemas aplicacionais tem por objectivo impedir a perda, alteração ou má utilização dos dados do utilizador nos sistemas aplicacionais, (Ferreira, 1995), este defende a segurança aplicacional na validação dos dados de entrada e processamento, técnicas de cifragem para protecção de dados sensíveis assim como mecanismos de autenticação. Dentro deste iten da segurança lógica, pode-se destacar a segurança nos seguintes pontos:

- Segurança dos Sistemas Aplicacionais
- Segurança dos Ficheiros dos Sistemas Aplicacionais
- Segurança nos Ambientes de Desenvolvimento e de Apoio Técnico

Requisitos de Segurança dos Sistemas Aplicacionais, tem como principal objectivo garantir a existência de mecanismos de segurança nos sistemas aplicacionais. Este tipo de segurança exige que requisitos de segurança aplicacional deve ser levada em consideração na fase da concepção da aplicação ou seja na fase do desenvolvimento. Para isso, há que existir a segurança no ambiente do desenvolvimento e nos trabalhos desenvolvidos.

Por conseguinte a segurança dos ficheiros dos sistemas aplicacionais deve garantir que os projectos das TI e as actividades de apoio técnico sejam conduzidas duma forma segura, por meio da segurança dos ficheiros, do controlo do suporte lógico operacional e da protecção dos dados de testes.

A Segurança nos Ambientes de Desenvolvimento e de Apoio Técnico, nesta óptica devem ser rigidamente controlados, de modo a assegurar que todas as alterações do sistema sejam analisadas para garantir que as mesmas não comprometem a segurança, quer do sistema aplicacional, quer do ambiente de protecção.

3.3.3.3 Gestão e controle de Acessos

O acesso aos sistemas informáticos deve ser controlados com base nos requisitos das actividades, dos utilizados, ou seja, condicionar o acesso ao sistema informático de acordo com a necessidade do utilizador. Cada sistema aplicacional deve estar subordinado a uma política de acesso claramente definida que estabeleça os direitos de acesso a cada utilizador ou grupo de utilizadores. Para isso devem ser levados em considerações os seguintes pontos:

- Gestão de Acesso de Utilizadores
- Controle de Acesso à Rede
- Controle de Acesso a Sistema Informático
- Controle de Acesso às Aplicações
- Monitorização do Acesso e Utilização do Sistema
- Monitorização da Utilização do Sistema

A Gestão de Acesso de Utilizadores, garante que as normas de acesso ao sistema informático sejam compridas, para isso deve existir um procedimento formal de registo e anulação de utilizadores para acesso a todos os serviços das (**TI**) multi-utilizador, a utilização de privilégios especiais deve ser controlada, a atribuição de *password* deve ser controlada rigidamente e os direitos de acesso dos utilizadores devem ser controlados regularmente. Dentro da gestão de acessos, (Ferreira, 1995), defende vários procedimentos:

- Registo de utilizadores
- Gestão de Passwords
- Gestão de Password de utilizador:
- Responsabilidades dos Utilizadores:
- Utilização de passwords:

Proteger os serviços conectados à rede é o principal objectivo do Controlo de Acesso à Rede, este controlo baseia-se no controlo de conexões aos serviços da rede, do percurso entre o terminal do utilizador e o sistema informático, de utilizadores remotos. Além destes controlos defenderem a autenticação dos utilizadores remotos aos sistemas informáticos e o acesso dos utilizadores devem ser controlados, a nível de:

- Serviços de Acesso limitado
- Autenticação do Utilizador
- Segurança dos Serviços de Rede

Impedir o acesso não autorizado ao sistema informático é o principal objectivo do controlo de acesso ao sistema informático. Acessos aos recursos do sistema informático devem ser controlados, sistemas de identificação automático dos terminais devem ser utilizados para autenticar conexões a locais específicos e terminais inactivos. Em áreas de alto risco, deve-se temporizar a utilização, para impedir acessos não autorizados, e restrições aos períodos de conexão devem ser efectuadas para proporcionar segurança adicional às aplicações de alto risco. Na perspectiva de Ferreira deve-se tomar algumas medidas como:

- Identificação do Terminal
- Procedimentos de “Logon” dos Terminais
- Identificadores do Utilizador
- Sistema de Gestão de Passwords
- “Time Aut “ Temporização do terminal
- Limitação do tempo de conexão

Impedir acessos não autorizados à informação residente nos sistemas informático é a principal função do controlo de acesso às aplicações. Restrição de acesso às informações, manipulação de utilitários do sistema, controlo de acesso à biblioteca de programa fonte e isolamento de sistema sensíveis são alguns procedimentos do controlo de acesso às aplicações. Dentro de controlo de acesso às aplicações pode-se levar em consideração os seguintes pontos:

- Restrição de acesso à informação
- Manipulação de Utilitários do Sistema
- Controlo de acesso às bibliotecas de Programa fonte

- Isolamento de Sistema Sensível

Na Monitorização do Acesso e Utilização do Sistema, a detecção de actividades não autorizadas é o seu principal papel, através da conservação dos ficheiros de auditoria relativos a segurança e a verificação da utilização do sistema.

Relativamente à Monitorização da Utilização do Sistema, são necessários os procedimentos para a monitorização da utilização do sistema, de modo a garantir que os utilizadores executem apenas os processos para os quais foram explicitamente autorizados. Deve-se avaliar os riscos em algumas áreas como a atribuição e utilização de contas com capacidade de acesso privilegiado e acessos fracassados ao sistema, (Ferreira, 1995).

3.4 A segurança nas Redes Universitárias

A segurança nas redes universitárias é algo que deve ser feita de forma contínua e activa, porque nas universidades existem utilizadores com perfis diferentes, que utilizam tecnologias diferentes, por isso é muito importante garantir a segurança nas redes universitárias, porque estes constituem numa forte ameaça.

- Para uma boa gestão da rede universitária, Ricardo Kleber ([S.D]), da Universidade de Federal do Rio Grande do Norte, defende a segurança em redes universitárias num sistema em camadas e nos seguintes níveis:
- Nivel 1: **Segurança nos Servidores**
- Nivel 2: **Segurança nos Activos de Rede I**
- Nivel 3**: Segurança na Administração**
- Nivel 4: **Segurança nos Postos de Trabalho**
- Nivel 5: **Segurança nos Utilizadores**
- Nivel 6: **Segurança nos Activos da Rede II**
- Nivel 7: **Segurança Física (Acesso a Pontos de Rede e Esquipamentos)**
- Nivel 8: **Segurança Física (Terrorismo, Espionagem, Sabotagem e Roubo)**

Na **segurança aos Servidores**, este defende que devem ser efectuadas actualizações/ configurações do sistemas operativos (S.O) com Packs, Patches e actualização do Kernel, actualização dos servidores com versões mais actualizadas possível do S.O para manter activos somente os serviços necessários e fechar portas abertas não utilizadas ou desnecessárias. Manutenção de Serviços "Críticos" com registo de "*Logs*", existência de planos de contingência através de servidores de ***backups*** (cópia de segurança) e simulação de sinistros.

Na **Segurança nos Activos de Rede,** como Hub e Switch, recomenda a preferencia por switch com a utilização de VLANs, utilização do DHCP e do IP fixo e separação físico e lógicos das subredes. Portas de Gestão com uso de detecção de intrusões, identificação de utilização das partas através do mapeamento.

Na **segurança na administração**, este defende que este tipo de segurança começa com a administração, por isso recomenda uma política de selecção de pessoal com "Ficha Limpa" em relação a crimes informáticos e participação na definição de políticas de segurança. Existência de planos de contingência para cada situações, programação em casos de paragem do funcionamento da rede através de avisos e comunicados previamente.

Na **Segurança nos Postos de Trabalho**, contra virus/Worms, spywares, utilização de permissão administrador/ Root, utilização de serviços sem criptografia (Telnet, HTTP, POP3 e SMTP).

Na **Segurança dos Utilizadores**, com políticas de segurança em relação a utilização de recursos, de regras de utilização de contas pessoais para funcionários a tempo inteiro, para utilizadores temporários, visitantes e funcionários que saíram da instituição. Proibição da Utilização de ferramentas para quebra de senhas.

Segurança nos **activos da Rede II** (Elementos do Roteamento), utilização do Firewall ou Listas de controlo de Acesso em equipamentos de roteamento.

E, Finalmente a **Segurança Física** em relação a pontos de rede e equipamento, defende activação quando necessário de pontos de rede nos corredores e configuração do time-out com a inactividade/bloqueio da contas de acesso. Em relação à segurança Física contra Terrorismo, Espionagem, Sabotagem e Roubo recomenda a colocação de câmaras vigilantes e sensores de movimentos e activação de alarmes. Recomenda também *backups* remotos de servidores principais assim como utilização de assinaturas hash de documentos electrónicos.

Capitulo 4 : A Auditoria Informática

O termo auditoria foi empregue incorrectamente, pois considerou-se que se tratava de uma avaliação cujo o único objectivo seria detectar erros e assinalar falhas,(carneiro, 2004). O conceito de auditoria, segundo este autor é mais amplo, podendo ser referido como um exame crítico que tem a finalidade de avaliar a eficácia e a eficiência de um departamento ou de uma organização.

Na perspectiva de Franco, (2001) a auditoria compreende o exame de documentos, livros e registos, inspecções e obtenção de informações internas e externas, relacionadas com o controle do património, objectivando mensurar a exactidão desses registos e das demonstrações contabilísticas deles decorrentes.

Na perspectiva de Carneiro, (2004) a auditoria é uma operação de análise e diagnóstico da empresa, tendo em consideração todos os aspectos da sua gestão, a fim de avaliar a coerência, a racionalização de processos e de apreciar a validade e o rigor dos resultados. De modo geral, a auditoria intervém em diversos domínios organizacionais, focalizando vários alvos ...”

4.1 Aspectos Históricos

A auditoria nasceu como um órgão de controlo de algumas entidades estatais e privadas. Inicialmente, a sua função não tinha carácter executivo e era estritamente de natureza económico-financeira, devendo manter-se absolutamente independente. Apesar de conter elementos de análise e de verificação, pode revelar sugestões de melhoria e até de planos de acção para eliminar essas disjunções e fraquezas, as quais são incluídas no relatório final sob o nome de recomendações, (carneiro, 2004).

Segundo de Franco, (2001) a auditoria surgiu como consequência da necessidade de confirmação dos registos contabilísticos, em virtude do aparecimento das grandes empresas e da taxa do imposto de renda, baseado nos resultados apurados em balanço. Sua evolução ocorreu paralelamente ao desenvolvimento económico, que gerou as grandes empresas, formadas por capitais de muitas pessoas, que têm na confirmação dos registos contabilísticos a protecção do seu património. A Inglaterra, que como denominadora dos mares e controladora do comércio mundial na época, foi o primeiro que surgiu coms grandes companhias de comércio e também a instituir a taxação do imposto de renda, baseado nos lucros das empresas. Além disso já se praticava neste país a auditoria das contas públicas, desde 1314, conforme a enciclopédia Britânica. O seu aparecimento como prática sistematizada, ocorreu somente no século XIX, pelo facto de somente a partir da segunda metade deste século é que começaram a surgir as primeiras associações de contabilistas públicos e profissionais que exercem as funções do auditor.

Na perspectiva de Carneiro, (2004) a auditoria enquanto actividade no âmbito do funcionamento empresarial, surgiu na Grã- Bretanha na segunda metade do século XIX no sentido de resolver problemas provenientes do desenvolvimento empresarial motivado pela revolução industrial. As invenções técnicas, os novos equipamentos, a utilização da energia eléctrica provocaram transformações tecnológicas e o número de empresas de algumas indústrias britânicas aumentou rapidamente, exigindo investimentos vultosos.

O número da dimensão empresarial, que atingiu rapidamente o aparecimento de sociedades anónimas, alterou o conceito de posse e propriedade, transformando os proprietários em accionistas que, como consequência dos seus investimentos, exigem que os gestores

apresentassem relatórios periódicos sobre o desenvolvimento e a rentabilidade dos seus negócios. Tendo em conta que os accionistas não tinham a possibilidade prática de analisarem as situações financeiras das suas empresa, apreciarem a utilização dos seus investimentos, os lucros ou os prejuízos contabilizados, tornou-se necessário designar técnicos habilitados a efectuarem essa análise de forma isenta, rigorosa e, portanto fiável, por ser possível a existência ou a inexistência de erros técnicos, de fraudes, de enganos devidos a omissões que pusessem em causa, os seus interesses financeiros. Esses técnicos foram denominados de auditores.

Iniciado deste modo, este tipo de auditoria (auditoria financeira), desenvolveu-se e teve aperfeiçoamentos, sobretudo, nos Estados Unidos da América do Norte e no Canadá, o que se deveu à respectiva evolução positiva de diversas indústrias transformadoras.

A auditoria hoje é uma nova forma de negócios no domínio de serviços. Realizada inicialmente por técnico externo e independente, a auditoria transformou-se num serviço prestado por empresas especializadas em diversos tipos de peritagem, as quais foram alargando as suas actividades para além da análise e avaliação do rigor das informações contabilístico-financeiras. Actualmente várias empresas prestam serviços nos domínios da auditoria, na acessoria fiscal, na consultadoria em Sistemas de Informação (SI), auxiliando assim muitas outras obras a manterem um dado nível de desempenho económico-social, no sentido de torná-las mais seguras, mais rentáveis e capazes de operar de modo competitivo, (carneiro, 2004).

4.2 Objectivo da auditoria

A auditoria, tem o objectivo de analisar o funcionamento parcelar ou global das organizações, para avaliar as deficiências de desempenho e sugerir vias de correcção e melhoramento. Por outro lado a auditoria não é uma actividade meramente técnica que implique apenas a aplicação de certos procedimentos cujos resultados apresentam um indubitável rigor. (carneiro, 2004).

A auditoria tem como objecto, inclusive, factos não registrados documentalmente, mas relatado por aqueles que exercem actividades relacionadas com o património administrado, cuja a informação mereça confiança, desde que tais informações possam ser admitidas como seguras pela evidência ou por indícios convincentes. Pode também basear-se em informações obtidas fora da empresa tais como as relativas à confirmação de contas de terceiros e de saldos bancários. Sobre esse objecto auditoria exerce a sua acção preventiva, saneadora e moralizadora, para confirmar a veracidade dos registros e a confiabilidade das comprovantes, com o fim de opinar sobre a adequação das situações e informações contidas nas demonstrações contáveis, na salvaguarda dos direitos dos proprietários, dos financiadores do património e da própria sociedade em geral.

4.3 Tipos de auditoria

Segundo Carneiro (2004)existem vários tipos de Auditoria:

Auditoria Externa – é uma auditoria realizada por entidades que não pertencem à organização auditada, tem o objectivo de clarificar a auditoria interna, devido a um maior distanciamento entre os auditores e os auditados. Esta auditoria destina-se a verificar se a situação financeira e os resultados das operações de um dado período são apresentados adequadamente pelas demonstrações financeiras e de acordo com as normas contabilísticas vigentes. Sendo esta auditoria elaborada por uma entidade imparcial, os resultados podem credibilizar a informação financeira perante entidades interessadas.

Auditoria Interna – Esta auditoria é realizada com recursos materiais e pessoas da empresa auditada e realiza-se perante uma expressa autorização dos órgãos máximos da mesma. Ela tem como propósito auxiliar a equipa de gestão no seu desempenho de atribuições e responsabilidades, com base nas suas avaliações e recomendações. Inicialmente pretendia-se que a auditoria interna preocupasse com a segurança dos activos da empresa, a detecção de fraudes e a credibilidade da informação financeira, obtida de acordo com os procedimentos determinados pelos órgãos de gestão. Actualmente, entende-se que a auditoria interna deve constituir uma função de avaliação independente, embora pertença à própria organização, que

tenha por finalidade o exame e a avaliação das suas actividades, constituindo assim num apoio à gestão empresarial.

Auditoria Operacional – É um aprofundamento da auditoria interna. O desenvolvimento das actividades empresariais fez com que, funções dos auditores internos passassem a incluir aspectos das diversas operações relacionadas com as actividades das várias áreas funcionais. O principal objectivo deste tipo de auditoria é avaliar a consecução dos objectivos e a economia dos métodos e dos procedimentos, identificando as irregularidade no sistema operacional. Compete-lhe analisar os métodos, procedimentos e sistemas de controlo para avaliar o cumprimento das orientações definidas, a eficiência da utilização dos recursos, a obtenção dos resultados pretendidos e ainda outros aspectos de carácter não financeiro das actividades da empresa. Este tipo de auditoria tende a apresentar propostas para a melhoria do desempenho empresarial, por isso procuram analisar a eficácia das operações e o cumprimento das políticas.

Auditoria de Gestão – Este tipo de auditoria realiza as suas actividades ao nível do planeamento estratégico, táctico e no processo decisório envolvido na aplicação de sistemas, políticas, critérios e procedimentos. Pode ser entendida como uma extensão da auditoria operacional. O objectivo deste tipo de auditoria é verificar em que medida é que os recursos (cada vez mais limitados) postos à disposição dos gestores estão a ser aplicados com a maior economicidade, eficiência e eficácia.

A auditoria de gestão ocupa de muitos temas de gestão, nomeadamente a definição de objectivos e a sua integração em políticas globais, o processo de planeamento e a sua tradução em programas de acções, a estrutura organizacional e a sua adequação com as políticas e os objectivos globais e finalmente a metodologia de controlo através da qual se deve avaliar os procedimentos empregues e os resultados obtidos.

Auditoria Financeira- Esta é realizada na área contabelístico-finaceira, tem por objectivo verificar a veracidade das situações financeiras, a adequação das operações e registos, a qualidade dos controlos internos, a observação das normas e regulamentos existentes e avaliar a correcta aplicação das normas e princípios contabilísticos vigentes.

No âmbito desta área, é importante a realização das seguintes análises.

- Assegurar a integridade e a adequação de todos os registos de natureza orçamental, financeira, económica e contabilística.
- Examinar e avaliar as aplicações de recursos, a respectiva rendibilidade e a sua contribuição para os resultados da organização, confirmando o cumprimento de normas legais, institucionais e aspectos contratuais.
- Considerar o valor dos objectivos das operações financeiras, nomeadamente investimentos, imobilizações, obrigações, despesas, receitas e fundos.
- Quando se trata de um auditor, acompanhar os trabalhos de auditoria financeira realizados por entidades independentes.

Auditoria de qualidade - Este tipo de auditoria é um processo de análise e avaliação segundo o qual se pretende verificar a eficácia desses sistemas quanto aos objectivos e padrões referidos. Podem ser classificadas de internas e externas:

- São internas quando ocorre por exemplo, a avaliação do plano de desenvolvimento do produto, para verificar o atendimento dos requisitos do cliente.
- São externas quando tem em vista a avaliação de fornecedores de matérias primas, de equipamento e/ou de serviço.

Auditoria Tecnológica – este tipo de auditoria tem por objectivo analisar as tecnologias mais importantes da cadeia de valor da organização, isto é, as tecnologias que mais influenciam a formulação de estratégias e a respectiva competitividade.

Neste tipo de auditoria, as tecnologias são analisadas quanto ao grau de adequação aos objectivos da organização, à sua gama de produtos e aos mercados onde a mesma opera. A auditoria tecnológica relaciona-se com duas situações:

- A primeira, os órgãos de gestão que pretendem averiguar se a utilização de diversas tecnologias está a decorrer de modo optimizado.
- A segunda, corresponde à decisão de adoptar novas tecnologias e ao processo de selecção, pois a modernização tecnológica deve ser integrada numa estratégia global.

4.4 A Auditoria Informática

Uma das transformações actuais mais significativas é a passagem de uma sociedade Industrial para a Sociedade de informação, onde o conhecimento é quase uma consequência directa. A informação e as tecnologias que lhe estão associadas representam alguns dos mais importantes activos das organizações. Tal como se exige para os outros activos, os requisitos de qualidade, controlos, segurança e actualizações são indispensáveis.

A informatização dos SI tem exigido profundas transformações, nomeadamente no que se refere à área financeira, aos procedimentos contabilísticos e aos respectivos sistemas de controlo interno. Apesar de grandes avanços tecnológicos, a situação actual dos SI em muitas pequenas e média empresas caracteriza-se por uma lenta assimilação das novas tecnologias, por uma insuficiência na utilização de equipamentos informáticos, pelo conservadorismo de muitos empresários e técnicos, por uma falta de planeamento dos SI e por soluções parciais que, por não estarem integradas, produzem situações de difícil controlo e manutenção.

Segundo Carneiro (2004)“ *a auditoria informática é um conjunto de procedimentos e de técnicas para avaliar e controlar total ou parcialmente um sistema informático*”.

Combinando conhecimentos do domínio computacional informáticos com os da gestão, a auditoria informática deverá estudar, examinar e avaliar periodicamente a evolução, através de metodologias e técnicas específicas, dos seguintes domínios:

- **Sistemas de Informação**: na âmbito do planeamento estratégico, na arquitectura dos SI e nas bases de dados e respectivos dicionários.
- **Infra-estrutura e das plataformas tecnológicas:** pode-se fazer no âmbito das configurações e das redes (tipificação, modelização e caracterização geral).
- Ferramentas e aplicações informáticas: no âmbito de sistemas de gestão das bases de dados, dos sistemas de apoio, dos geradores e editores de programas.

A auditoria informática comporta a análise, validação e avaliação do controlo interno de sistemas de informação e estes integram um conjunto de recursos: humanos, materiais, tecnológicos e financeiros, que integram de acordo com uma sequência lógica a fim de transformarem dados obtidos em informações que auxiliam na tomada de decisões.

4.4.1 Tipos de Auditoria Informática

A auditoria informática examina uma parte do sistema informático já em exploração (condições operacionais, procedimentos de controlo e resultados proporcionados), deve intervir em fases anteriores à exploração, sobretudo em situações de alterações de todo o sistema. Em autoria informática, nas análises e avaliações são adoptados os mesmos princípios da auditoria geral, no entanto tem algumas diferenciações. Por exemplo:

- No âmbito das necessidades em investimentos de hardware e software - chamada de auditoria dos investimentos informáticos,
- Na protecção dos sistemas informáticos nos seus aspectos físicos e lógicos - chamada de auditoria de **segurança informática**,
- Nas alterações estruturais na função informática - chamada de **auditoria de organização informática**.

Em casos da auditoria no domínio de desenvolvimento de projectos de informática de uma empresa, faz-se uma integração dos três tipos de auditoria.

Existem outros tipos de auditoria informática segundo as consultas efectuadas no site, a seguir

o site http://www.monografias.com/trabajos5/audi/audi.shtml,

Auditoria informática de sistemas: Este tipo de auditoria faz a revisão dos sistemas de informação, tanto a nível do *hardware* e de *software*, com o objectivo de procurar potenciais melhorias e determinar como poderia actuar de modo a melhorar este aspecto.

Exploração: Faz a revisão de todos os processos encarregados de produzir resultados, entre a captura de informação, os sistemas de hardware de exploração, os recursos humanos de exploração e de entre outros.

Comunicação: Revisão da topologia de rede e determinação de possíveis melhorias, análise de rede e gralhas de utilização.

Desenvolvimento de Projectos: Revisão completo de processos de desenvolvimentos de projectos por parte da empresa aditada. Esta análise se baseia em 4 aspectos fundamentais:

- Revisão das metodologias utilizadas.
- Controlo interno das aplicações.
- Satisfação dos utilizadores.
- Controlo dos processos e execução de programas críticos.

Segurança: Abarca os conceitos de segurança física e lógica. A segurança física se refere a protecção de hardware e dos suportes de dados, assim como dos edifícios e instalações que se abarcam, contemplando as situações de incêndios, sabotagens, roubos, catástrofe natural e etc.

4.4.2 Porquê Auditar

A sobrevivência e o crescimento das organizações dependem das suas capacidades de se relacionarem com as envolventes em que se inserem. Tanto na envolvente transaccional como na contextual, vão acontecendo muitas modificações que influenciam os comportamentos organizacionais nas suas relações com os mercados onde operam. Essas capacidades de

relacionamento dependem, por sua vez, da recolha e do tratamento de dados, a fim de transformá-los em informações capazes de fundamentarem decisões estratégicas.

As empresas, através dos seus técnicos e das sua s áreas funcionais utilizam ora os dados dispersos, ora a informação já organizada para fundamentarem a formulação das suas estratégias. Nem sempre os órgãos de gestão dispõem de uma informação completa sobre os novos acontecimentos e sobre mudanças ocorridas nas envolventes transaccional ou contextuais, mas podem procurar diversos tipos de informação adicional para conseguirem tomar melhores decisões.

Segundo Carneiro (2004)as empresas devem considerar que as suas actuações não são independentes, existindo, frequentemente, relações cruzadas entre os diversos componentes do meio envolvente que condicionam as análises, as formulações e as implementações de estratégias. Actualmente, o funcionamento de muitas empresas públicas e privadas necessita da tecnologia de teleprocessamento electrónico de dados, pelo que temos hardware e software e as suas implicações práticas estão já incluídas na cultura organizacional e consequentemente no dia-a-dia desses empresas. Neste óptica o tecido económico vai, cada vez mais, aconselhando a efectivação da auditoria dos SI informatizados, quer desempenhada por técnicos internos quer requerendo a intervenção de empresas especializadas.

A auditoria dos SI informatizados torna-se numa ferramenta de gestão das direcções das empresas, sendo também útil aos accionistas e as entidades externas no sentido de avaliar e validar a qualidade das operações que utilizam as tecnologias do equipamento informático. É notório que o ambiente empresarial vai acompanhando a evolução tecnológica do processamento de dados e recorrendo a necessidade da função de auditoria informática.

A informática enquanto, sistema que integra diversas tecnologias, está sendo utilizada por quase todos os agentes económicos dos países mais desenvolvidos ou em vias de desenvolvimento. Segundo Carneiro (2004) os SI e os respectivos equipamentos deveriam estar sujeitos a um controlo regular a fim de garantir a sua segurança. Este refere alguns motivos desta necessidade: Os computadores e os centros de processamento de dados podem

ser meios úteis à espionagem industrial, Apresentação de dados incorrectos por alguns SI deficiente, que pode converter-se numa ferramenta perigosa para a empresa.

Este autor ainda faz referência a aspectos que permitem garantir a segurança dos SI nomeadamente a necessidade de uma auditoria informática devido a razões como a descoordenação e desorganização quando os objectivos da função informática não compatibilizam com os globais da organização, a deficiente imagem e insatisfação dos utilizadores e a insegurança, onde é aconselhável fazer uma avaliação do nível de risco no que se refere à segurança física e lógica.

4.4.3 Finalidade da Auditoria Informática

A auditoria informática tem as seguintes finalidades:

- Proteger as actividades da empresa e os seus recursos, confirmar se o hardware e o software que se pretende adquirir corresponde inteiramente às necessidades da empresa.
- Garantir o controlo da função informática,
- Analisar a eficiência dos sistemas informáticos,
- Verificar as condições em que ocorre a exploração dos procedimentos de controlo e os processos de segurança inerentes, no que respeita a *hardwares, sof*twares, dados, informações e o pessoal,
- Verificar o cumprimento das normas gerais da empresa no que se refere à função informática.

4.4.4 Relações da auditoria informática e o controlo Interno

O controlo interno informático e a auditoria informática têm algumas analogias. Alguns auditores informáticos passaram para o domínio do controlo interna informático devido às semelhanças dos objectivos profissionais de controlo interno e a auditoria.

No que concerne às semelhanças entre o controlo interno informático e a auditoria informática, pode-se dizer que existe em ambos, pessoal interno com conhecimento especializados em tecnologias da informação, com o propósito de verificar o cumprimento de controlos internos, de acordo com procedimentos estabelecidos para os sistemas de informação.

No que concerne às diferenças, o pessoal do controlo interno informático faz a analise dos controlos no dia-a-dia, o alcance das suas funções abrange apenas os objectivos do departamento de informática e reporta apenas à Direcção do departamento de informática. Enquanto que a auditoria informática abrange o pessoal interno e externo, a análise é feita num dado momento, cobre todos os componentes dos sistemas de informação e repota à direcção geral da empresa.

4.4.5 Características do Auditor Informático

Todas as organizações, incluindo Universidades, ministérios, hospitais, tendem a utilizar a informática para gerir as suas actividades de modo a atingirem os seus objectivos.

O auditor informático tem a função de emitir juízo global ou parcial baseados em factos e situações, com o intuito de cuidar da correcta utilização de todos os recursos que a organização utiliza para poder dispor de um sistema de informação suficientemente eficiente e eficaz. Na sua interacção com a empresa e com o responsável da área a ser auditada, o auditor deve tomar muito cuidado devido às características psicológicas do auditado, dado que tem necessidade de realizar o seu trabalho com profissionalismo e eficiência.

É muito importante que um auditor informático domine técnicas de auditoria, sistemas de informação e de processamento electrónico de dados, ainda deve ter alguma preocupação de ir actualizando os seus conhecimentos no decorrer da sua carreira profissional, procurando especializar-se mais em determinadas áreas computacionais do que nas outras.

Também é muito importante que um auditor tenha algumas aptidões e característica psicológicas no domínio da personalidade profissional como: Honestidade e Integridade moral, objectividade independente das influências que outros possam pretender exercer, aptidão crítica para identificar insuficiências e problemas, exigências de rigor nos seus processos de trabalho, flexibilidade que permita maior adaptação às situações, autocontrole emocional, para poder suportar situações de tenção e de entre outros aspectos.

4.4.6 Principais técnicas de Análise e de Controlo

Um auditor informático para realizar as suas funções, dispõe de um conjunto de técnicas adequadas para tal. A aplicação desses técnicas implica que sejam considerados elementos como o parâmetro do controlo interno a ser analisado, as condições tecnológicas em que irá ser efectuada a aplicação e a natureza dinâmica da situação do sistema. Esta situação pode estar de entre esses três tipos: Auditoria do Sistema em operação, do sistema em desenvolvimento e do centro de processamento de dados.

Dependendo das situações de aplicação, assim será a aplicação das vária técnicas utilizadas para recolher as informações, essas podem ser: Questionários, Entrevistas, Checklist.

Questionários

As auditorias informáticas baseiam-se em informações oral e documental de todos os tipos e recebidas por fontes e é sobre estes pilares e com o suporte de factos demostráveis e/ou evidentes, que o auditor consegue fundamentar a emissão de um juízo global objectivo. O auditor pode começar por solicitar o preenchimento de questionários, previamente impressos e enviados aos responsáveis das diversas áreas a auditar, podendo o mesmo envio ser também feito para utilizadores de outros níveis. Este segundo, deve ser cuidadosamente elaborados quer em conteúdos quer na forma, e deve ser elaborado de acordo com especificidade de cada situação.

Entrevistas

As entrevistas são uma das formas que o auditor utilizada para obter informações relevante para o seu processo de análise. Podem ser dirigidas de forma aberta ou semi-dirigidas, para que o entrevistado forneça todos os dados que lhe pareçam ter alguma relação com o tema em causa e para que o auditor possa registar dados que complemente informações que não são adquiridas em meios puramente técnicos ou pelas respostas dos questionários. Este tipo de técnicas deve ser preparado de acordo com cada situação envolvente e o auditor deve segundo Carneiro (2004)procurar alcançar uma conversa o menos tensa possível de modo que o entrevistado responda com simplicidade as perguntas, fornecendo sempre os dados importantes que permita alcançar os seus objectivos.

Checklist

O auditor reelabora os questionário em função das situações que encontra. O auditor segundo Carneiro (2004)deve construir perguntas muito estudadas e de formulação flexível, que o permite obter respostas coerentes que permitam uma correcta descrição dos pontos fracos e fortes. Esse conjunto de perguntas tem o nome de *checklist*. Os checklists devem ser respondidas oralmente, pois podem fornecer conteúdos mais individualizados e mais ricos do que as outras perguntas, estas *checklists* podem ser com escalas de avaliação ou com perguntas fechadas.

Capitulo 5 : O caso das Instituições de Ensino Superior em Cabo Verde

5.1 Enquadramento

A República de Cabo Verde é um arquipélago constituído por 10 ilhas e alguns ilhéus, situada na costa ocidental africana, com uma superfície terrestre de 4033 Km2 e uma população de aproximadamente 75000 mil habitantes. Tendo um clima tropical seco, faz parte do grupo de países do Sahel região particularmente afectada pela seca e desertificação.

Cabo Verde é actualmente considerado um país de desenvolvimento médio, contando com uma taxa de analfabetismo de 25,2% e com uma taxa de electrificação de 80%. É o 29º País Africano que obteve ligação à Internet, em 1996. Segundo os dados do Instituto Nacional de Estatística (INE)[10] , a penetração do telefone é de 51%, do telemóvel é de 20% e a posse do computador com acesso à Internet é de 2,3% aumentando a cada dia. A nível de África, a utilização de novas tecnologias em Cabo Verde está num nível encarado como bastante aceitável.

O Ensino Superior em Cabo Verde é muito recente, teve o seu início em 1979 com a criação da escola de formação de Professores – Actual Instituto Superior de Educação. Actualmente

[10] Instituto Nacional de Estatística, www.ine.cv

dispõe de 6 instituições de ensino superior com um total 5200 estudantes, o que constitui 20% do total de acesso ao ensino superior em Cabo Verde.

Este estudo debruçou-se sobre o estado da utilização da tecnologia de Informação e Comunicação nas Instituições de Ensino Superior cabo-verdiana de modo a saber qual é a sua influência no binómio Ensino-Pesquisa no seio dessas instituições.

O **objectivo geral** do estudo é perceber o panorama da utilização de tecnologias de redes, a segurança e a auditoria de redes no contexto das instituições de ensino superior em Cabo Verde.

Os **objectivos específicos** são:

- Entender a Estrutura da Rede nessas instituições.
- Estudar a utilização das Tecnologias de Informação e Comunicação dessas instituições.
- Analisar algumas práticas de Segurança da Informação.
- E conhecer a visão dos administradores de rede em relação às Tecnologias de Informação e Comunicação e à segurança da informação.

O estudo teve como **perguntas de partida**:

- Qual é a importância e o contributo das Novas Tecnologias numa Instituição de Ensino Superior.
- Quais são as tendências de utilização das Tecnologias de Informação e Comunicação e as práticas da segurança e auditoria da informação nas instituições de ensino superior em Cabo Verde?

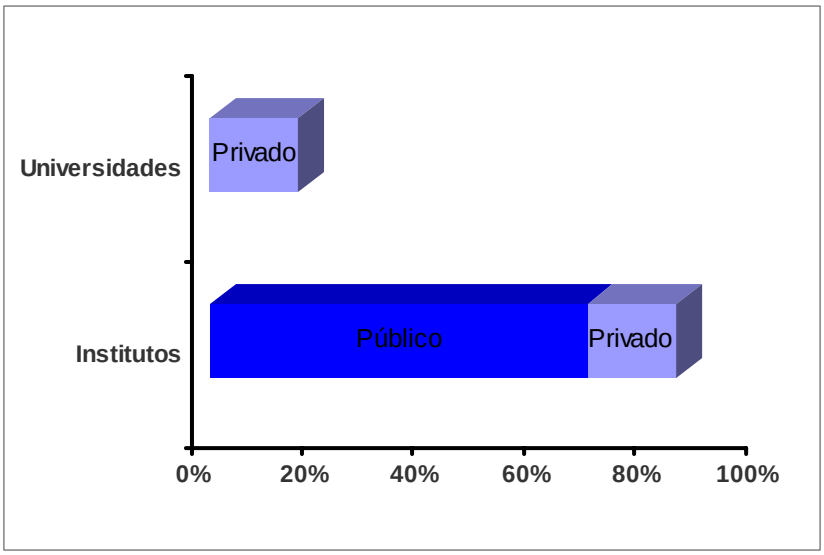
A **investigação** teve como suporte:

- A distribuição de 2 formulários no intuito de obter os informações de segurança e de auditoria informática nas 5 de 6 instituições de ensino existentes.
- Análise dos dados.

5.2 Caracterização da Amostra

Cabo Verde dispõe actualmente de 6 Instituições de Ensino Superior. Estas instituições estão sediadas nas ilhas de Santiago e São Vicente e são de domínio público e privado. Segundo os dados obtidos no estudo, as instituições públicas constituem quase 70% dos institutos existentes em Cabo Verde.

Gráfico 1 - Instituições de Ensino Superior em Cabo Verde



O Ensino Superior em Cabo Verde é muito recente, tendo o seu início no ano 1979 com a criação da Escola de Formação de Professoes - Actual Instituto Superior de Educação (ISE) e posteriormente em 1994 o ISECMAR (Instituto Superior de Engenharia e Ciências do Mar) e em 1991 do ISCEE (Instituto Superior de Ciências Económicas e Empresariais).

Mais recentemente, a crescente procura de ensino superior no país devido à escassez de bolsas e vagas para estudos no exterior, motivou a criação de duas instituições privadas de ensino superior, a Universidade Jean Piaget de Cabo Verde, no ano 2001 e o IESIG (Instituto de Ensino Superior Isidoro Graça), em 2002.

Para além destas instituições, existe o INIDA (Instituto Nacional de Investigação e Desenvolvimento Agrário) que é a instituição com mais projectos de investigação científica a nível nacional.

O universo de estudo abrangeu 5 Instituições de Ensino Superior sediadas tanto na Praia como no Mindelo, o que constitui 83% do total da amostra.

Para alcançar os objectivos delineados neste trabalho, foram feitos dois questionários: Um primeiro com o fito de avaliar as tecnologias de informação e comunicação utilizadas para o ensino-pesquisa, e um segundo visando avaliar a rede e algumas práticas de segurança nessas instituições.

O **primeiro questionário** teve quatro grupos de perguntas com a finalidade de estudar os seguintes aspectos: a utilização das tecnologias de informação e comunicação para o ensino; a estrutura da rede; a segurança e auditoria da informação; e a análise das sensibilidades dos inquiridos no que diz respeito à segurança.

O **segundo questionário** serviu de complemento ao primeiro, tendo em conta a sensibilidade do tipo de perguntas colocadas. Este teve também quatro grupos de perguntas que avaliam os seguintes aspectos: os requisitos das redes; a utilização dos recursos disponíveis nas redes; o estado da implementação da segurança; e a avaliação interna por parte dos inquiridos sobre alguns aspectos relacionados com as novas tecnologias (vide o anexo **I** e **II**).

A metodologia utilizada para a materialização deste estudo baseou-se em inquéritos. Num primeiro momento fez-se a distribuição dos formulários em relação a alguns aspectos respondidos nos questionários e que serviram de suporte para a construção do segundo questionário.

.

Durante as interacções havidas com os vários inquiridos nesse estudo, manifestaram o facto do questionário apresentado ter-lhes despertado atenção para alguns problemas de segurança que até então negligenciavam, tendo mesmo solicitado exemplares do mesmo para eventual aproveitamento futuro, em termos de melhoria da segurança nas respectivas instituições.

A análise dos resultados conseguidos nos inquéritos foi feita em duas fases:

- Na primeira fase os dados recolhidos serviram para entender a utilização das Tecnologias de Informação e Comunicação nas Instituições de Ensino Superior Cabo-verdianas
- Na segunda fase os dados recolhidos serviram para avaliar o Estado da Segurança da Informação nessas Instituições.

5.3 Análise dos Resultados

5.3.1 A Utilização das Tecnologias de Informação E Comunicação

Nesta secção pretende-se mostrar os resultados obtidos de alguns indicadores como: a infa-estrutura da rede nas instituições de ensino em Cabo Verde; a existência de Tecnologias de Informação e Comunicação; a Taxa de Utilização dessas Tecnologias; e as Tecnologias utilizadas para o ensino universitário face às actuais exigências do processo de ensino e pesquisa.

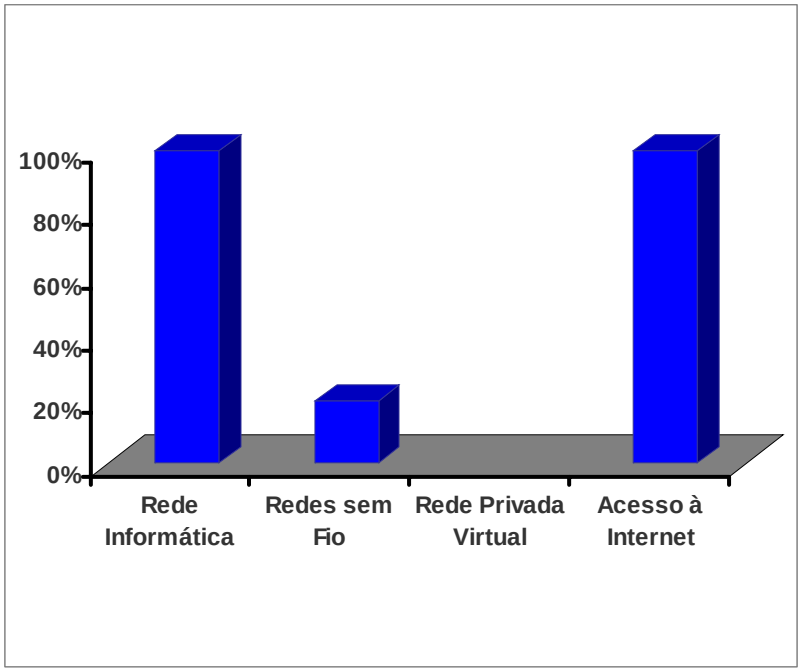
5.3.1.1 As Infra-Estruturas de Rede

Os resultados obtidos na avaliação da infra-estrutura de redes nas instituições de ensino superior em Cabo Verde estão apresentados no gráfico 2.

Segundo estes resultados, 100% das instituições de ensino superior em Cabo Verde têm infra-estrutura de redes, com acesso à Internet, o que constitui num indicador muito positivo tendo em conta que o acesso à Internet é fundamental para a qualidade de ensino, por fornecer fontes de pesquisas que ultrapassam barreiras geográficas, temporal e cultural.

Embora exista a rede e o acesso à Internet em todas as instituições, não existe a flexibilidade de acesso dentro dessas instituições no sentido de colmatar o problema da mobilidade dos utilizadores, como se prova pela inexistência de redes sem fio em quase todas as instituições, onde apenas 20% tem redes sem fio, só para acesso interno e 100% não tem a possibilidade do acesso remoto a partir de ambientes externos à instituição.

Gráfico 2 - Infra-estrutura da Redes nas Instituições



Em relação aos tipos de ligações mais utilizadas nessas instituições destacam o ADSL(Asymmetric Digital Subscriber Line_) e ISDN(Integrated Services Digital Network_), com velocidades variando de 64 Kbps até 1024 Mbps.

Tabela 1 - Tipos de ligação e larguras de banda

Tipo de Ligação	Largura de Banda				
	64 Kbps	128 Kbps	11 Mbps	256 Mbps	>= 512 Mbps
ISDN	12,5%	37%			
ADSL				25%	12,5%
Wireless via NOSE			12,5%		

Os dados apresentados na tabela 1, mostram que 12,5% das instituições utilizam ISDN de 64 e 37% de 128 Kbps, 12,5% utilizam Wireless via Nose de 11 Mbps, e 37,5% utilizam ADSL, onde 12,5% tem linha de 256 Mbps e 25,5% acima de 1024 Mbps.

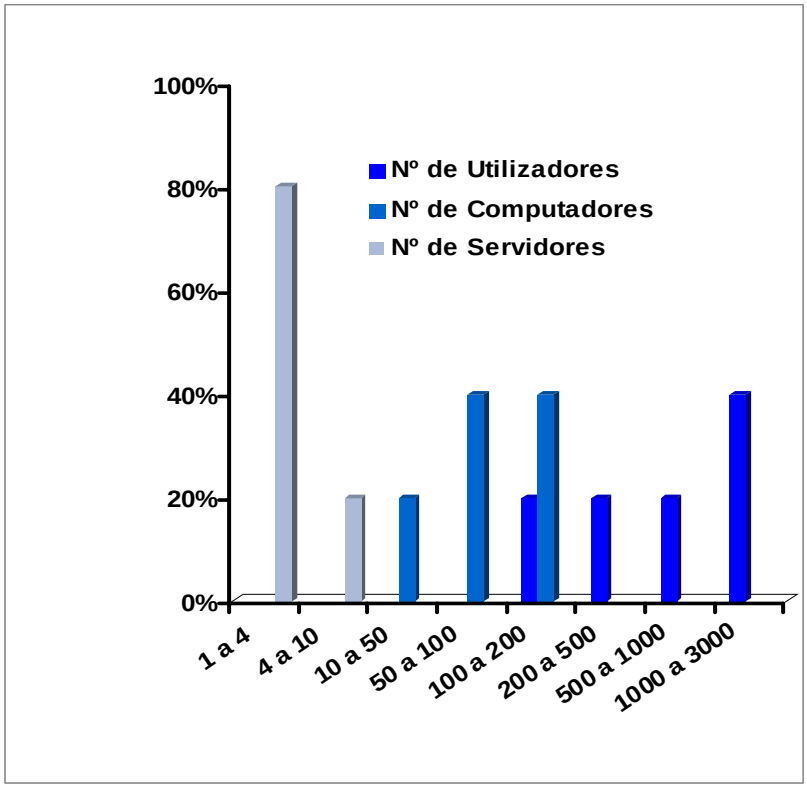
Estas ligações indicam que a maioria das instituições não tem grandes demandas de tráfico e, por conseguinte, serviços que exigem grande quantidade de largura de banda. As características destas ligações indicam que em algumas instituições o ISDN é utilizado como linha de *backup*, uma vez que algumas instituições públicas estão ligadas à rede do Estado, o que significa que o acesso à Internet depende em grande parte da ligação à essa rede porque o ISDN utilizado não suporta as suas exigências internas. O facto da maior parte das instituições utilizarem o ADSL dado que esta se trata de uma linha de banda larga com altas velocidades, é significativo, e muito positivo.

5.3.1.2 Tecnologias de Informação e Comunicação

As tecnologias de informação e comunicação constituem, nos dias de hoje, uma ferramenta essencial para qualquer organização, porque permitem uma maior produtividade dos seus colaboradores e uma maior qualidade no oferecimento dos seus bens e serviços. Nesta secção mostram-se os resultados obtidos em relação a alguns indicadores que caracterizam uma rede local.

No gráfico 4, pode-se observar que o número aproximado de Utilizadores varia entre 100 a 3000, o de Computadores varia entre 50 a 200 e de Servidores varia de 1 a 10. Esses resultados mostram que a maior percentagem de estudantes universitários não utilizam os recursos da rede disponibilizados, porque o número de computadores e servidores que existem demonstram claramente que se todos eles utilizassem a rede diariamente esses recursos seriam insuficientes e não cobreariam as necessidades dessas instituições, uma vez que em redes de 1000 a 3000 alunos, apenas uma percentagem abaixo dos 50% é que utilizam os recursos disponibilizados na rede.

Gráfico 3 - Estatística do número de Utilizadores, Computadores e Servidores



Além desses indicadores, pode-se constatar, na tabela 2, aspectos como a competência dos utilizadores, capacidade dos computadores, Sistemas Operativos utilizados e tipos de servidores existentes nessas instituições.

Tabela 2 - Estatística de alguns Recursos da Rede

Recursos	**Percentagem (Total = 100%)**			
Utilizadores	**Inexperientes**	**Com alguma dificuldade**	**Razoáveis**	**Competentes**
	19%	38%	28,6%	14,4%
Sistemas Operativos	***Windows***	***Linux***	***Mac***	**Outros**
	90,8%	7,2%	1%	1%
Computadores	**Lentos**	**Razoáveis**	**Rápidos**	
	13,4%	42%	41%	
Servidores	**Dados**	***web***	**Outros**	
	100%	70%	50%	

Nesta tabela, pode-se verificar que a competência do grosso dos utilizadores é **(com alguma dificuldade)**, o que significa que a maior percentagem não detêm competências/recursos para

lidar com certos tipos de ferramentas e não utilizam convenientemente os recursos que lhes são disponíveis.

Tendo em consideração que a maior parte dos computadores existentes nessas instituições são considerados razoáveis e rápidos, este indicador mostra que é necessário uma maior dinâmica nessas organizações para um melhor aproveitamento das vantagens que os recursos tecnológicos podem oferecer no seio dessas instituições, principalmente no acesso a informações. Em relação ao sistema operativo utilizado, quase 100% das instituições utilizam o *Windows,* o que mostra uma certa dependência em relação à *Microsoft*, e uma semelhança dos serviços e recursos disponíveis nessas redes.

No que diz respeito a tipos de servidores, 100% das instituições tem servidores de dados, 70% utilizam servidores *WEB* e 50% utilizam outros tipos de servidores. Este indicador nos mostra facilmente que os serviços que existem nessas redes são essencialmente o acesso à Internet e a dados, o que demostra nitidamente alguma insuficiência na utilização de tecnologias comparativamente a outras universidades como, por exemplo, na uso do serviço de correio electrónico institucional e de *web hosting*.

5.3.1.3 Taxa de utilização dos Recursos

É ponto assente de que ter tecnologias numa organização não é suficiente, já que o mais importante é saber tirar o proveito destes investimentos e averiguar como é que os utilizadores tiram proveito dessas tecnologias, na medida em que investir em novas tecnologias e não tê-las disponíveis é, na prática, como se não os tivesse. Nesta óptica, analisa-se, nesta secção, a utilização dos recursos. Segundo os resultados da tabela 3 faz referência à utilização dos computadores e da Internet e, observou-se que um número significativo dos utilizadores (80%) tem acesso aos computadores e 60% utiliza do computador para trabalhar. Em relação à Internet, um número significativo tem acesso à Internet (60%) e utilizam o correio electrónico (60%).

Em relação aos recursos da Internet, os dados estatísticos apontam que uma média de 60% de utilizadores não utiliza este serviço da melhor forma uma vez que o nível de procura de informação e recursos na Internet é muito baixa, sendo que a maioria das pessoas utilizam apenas o correio electrónico.

Tabela 3 - Avaliação da Taxa de acesso de alguns recursos tecnológicos

Utilização dos recursos da Rede	Percentagem das Pessoas que Utilizam essas Tecnologias			
	Ninguém	Alguns	N.º Significativo	Todos
Acesso ao Computador			80%	20%
Acesso ao Computador para trabalho		10%	60%	10%
Acesso à Internet		20%	60%	20%
Acesso a serviços de Correio Electrónico		20%	60%	20%
Acesso aos recursos da Internet		60%	40%	

Os dados da tabela 3 mostram que é necessário ainda um muito maior investimento na formação dos utilizadores nessas instituições. Colocar um computador a disposição do utilizador não significa, automaticamente, o aumento da produtividade deste caso não saiba tirar proveito das ferramentas que lhe são disponibilizadas. Quanto aos dados da utilização dos recursos da Internet, 60% tiram o proveito mínimo destes recursos, significando que a maior parte dos utilizadores dentro das instituições tem conhecimentos apenas na óptica do utilizador, e que pouco proveito está a ser retirado dessas novas tecnologias para as pesquisas em função do ensino-aprendizagem. Mas a taxa de utilização do acesso a recursos não é medida somente através destes indicadores, é necessário saber que recursos são disponibilizados, e se correspondem ou não às necessidades dos seus utilizadores.

Em relação aos recursos disponibilizados, a tabela 4 faz referência à percentagem dos utilizadores que utilizam recursos como serviços de impressão, acesso a dados e a utilização de algumas ferramentas para trabalho.

Tabela 4 - Avaliação da taxa de utilização dos recursos disponibilizados na rede

Recursos Utilizados	Percentagem das Pessoas que utilizam essas Tecnologias			
	Ninguém	Alguns	Nº significativo	Todos
Serviços de impressão		20%	40%	40%
Acesso a pastas partilhadas		60%	20%	20%
Acesso a base de dados		100%		
Acesso a Sistemas de Informação	20%	60%	20%	
Ferramentas do Office			80%	20%
Ferramentas específicas		80%		
Programas de tratamentos de dados		80%	20%	
Motor de busca		60%	20%	20%

Nesta tabela pode-se observar que as instituições inquiridas têm acesso a serviços de impressão e estas estão/são disponibilizadas para quase 100% dos seus utilizadores. Em relação ao acesso a base de dados, 100% das instituições afirmam que alguns é que têm acesso a base de dados, o que demonstra que os dados não estão relacionados apesar de existir computadores em redes e que, pelo facto de não utilizarem um sistema de informação académica para trabalhar, torna-se muito complicado fazer a gestão académica dos estudantes, das disciplinas e dos cursos. A próxima secção incidirá sobre este aspecto de forma particular.

Estes indicadores apontam que em todas as instituições inquiridas, em termos de recursos da rede, se utiliza os serviços básicos, comuns à uma organização. Uma instituição de ensino superior deve ter os recursos tecnológicos mais avançados possíveis devido às exigências da estrutura orgânica dessas instituições.

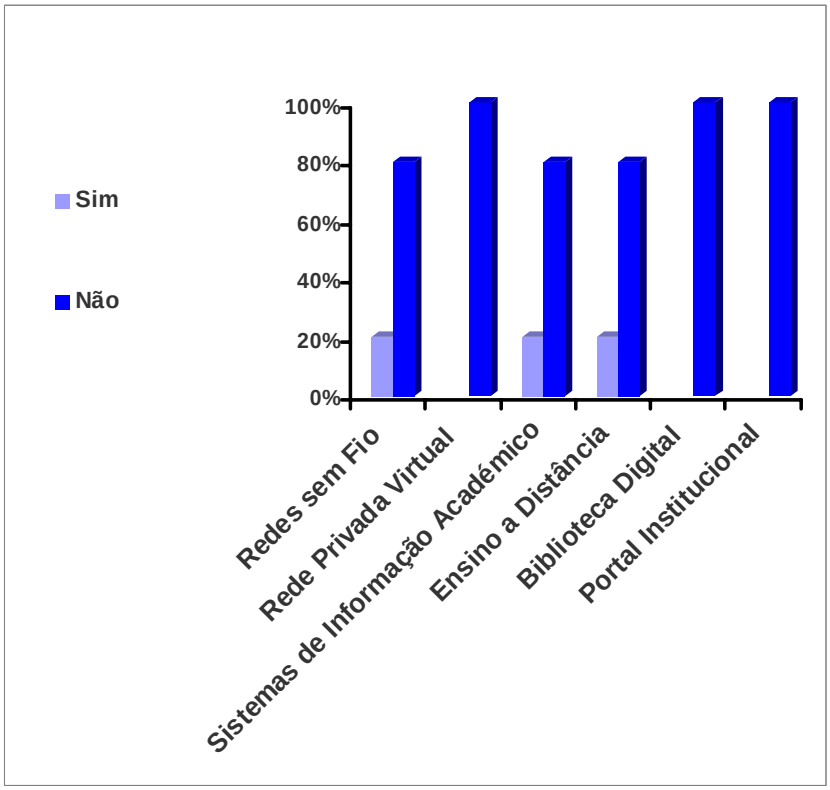
5.3.1.4 Tecnologias para o Ensino Universitário

Numa rede, não basta ter recursos como computador, impressora e acesso à Internet. É necessário procurar mecanismos onde se consegue tirar o máximo proveito desses recursos, de modo a que os investimentos realizados possam compensar.

No gráfico 4, foram levados em consideração a existência de tecnologias como rede sem fio, rede privada virtual, sistemas de informação académica, ensino a distância, biblioteca digital e

portal institucional, com o intuito de entender como é que as instituições de ensino superior cabo-verdianas estão a utilizar as tecnologias de informação e comunicação para tirar proveito da tecnologia de rede para o processo de ensino-aprendizagem e projectos de investigação.

Gráfico 4 - Taxa de existência de alguns Recursos para o Ensino



No gráfico, pode-se observar e confirmar que em relação às redes sem fio, estas não existem em 80% das instituições de ensino superior, o que não flexibiliza a mobilidade de acesso aos utilizadores, por exemplo, com computadores portátil. Caso uma instituição tenha alguns recursos indisponíveis, como, por exemplo, laboratórios de informática, que não existem em grandes números segundo os dados obtidos, os alunos poderiam utilizar os seus computadores portáteis em qualquer lugar dentro das instituições.

Perante o facto de um estudante ter computador e acesso à Internet em sua residência, a possibilidade de aceder aos recursos a partir da mesma afigura-se impossível, uma vez que 100% das instituições não permitem esse serviço, pela inexistência da rede privada virtual. Isto significa que quando um aluno precisar de qualquer recurso da escola, tem que recorrer a esse estabelecimento fisicamente.

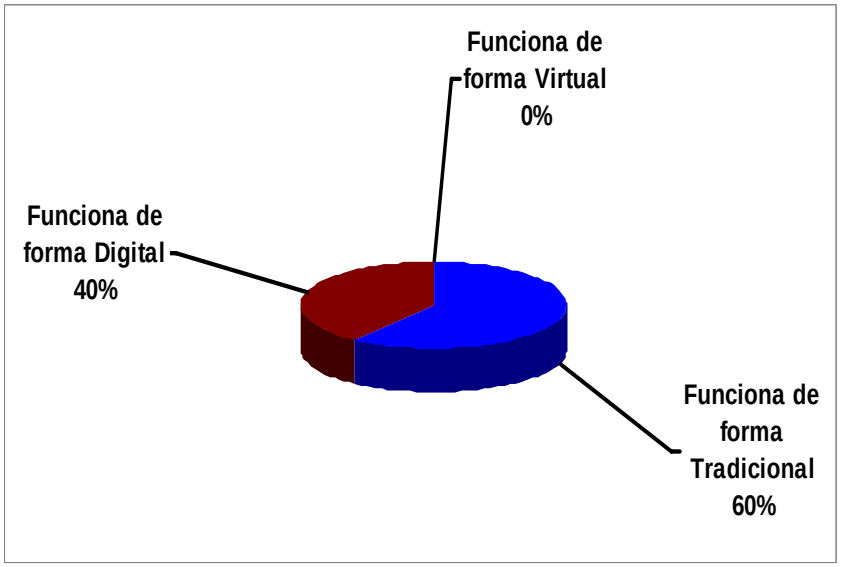
Em relação à gestão das informações académicas como: alunos, docentes, horários, cursos e disciplinas, em 80% das instituições não existe um sistema de informação académica para gerir este problema, sendo que a maioria utiliza ficheiros *word (microsoft office)* com essas informações, o que repercute de alguma forma na gestão dos cursos ministrados nessas instituições. Esse indicador mostra que a gestão dos serviços académicos está a ser feita duma forma muito tradicional e pouco eficiente, por não existir uma base de dados com relação de alunos com cursos, disciplinas e docentes, nem docentes com cursos, disciplinas e carga horária.

No que refere às tecnologias de ensino, no caso de assim o podermos denominar, nomeadamente Ensino a Distância, Biblioteca Digital e Portal Académico, observou que a existência dessas tecnologias levará algum tempo para se efectivar, tendo em atenção que 80% das instituições não têm recursos de ensino a distância e que 100% das mesmas não dispõem de biblioteca digital e de portal académico, recursos que permitem o acesso mesmo em ambientes fora da instituição.

Levando em consideração as vantagens duma biblioteca digital, por exemplo a possibilidade de acesso a recursos bibliográficos, do ensino a distância pela facilidade de acesso a recursos didácticos e partilha de conhecimentos a distância, do portal universitário por permitir a realização de muitos processos burocráticos a distância, pode-se reconhecer que as instituições de ensino superior analisadas precisam de uma de revolução na utilização de novas tecnologias, para que o corpo docente e discente possam tirar maior proveitos dos recursos de ensino-aprendigem existentes actualmente.

Diante desses dados constatou-se que a maior parte das instituições de Ensino Superior em Cabo Verde funcionam duma forma arcaica, desperdiçando assim as vantagens dum funcionamento digital e/ou virtual. O gráfico 6 mostra a classificação dos inquiridos quanto ao funcionamento das suas instituições.

Gráfico 5 - Forma de funcionamento dessas instituições



5.3.2 Estado da Segurança da Informação

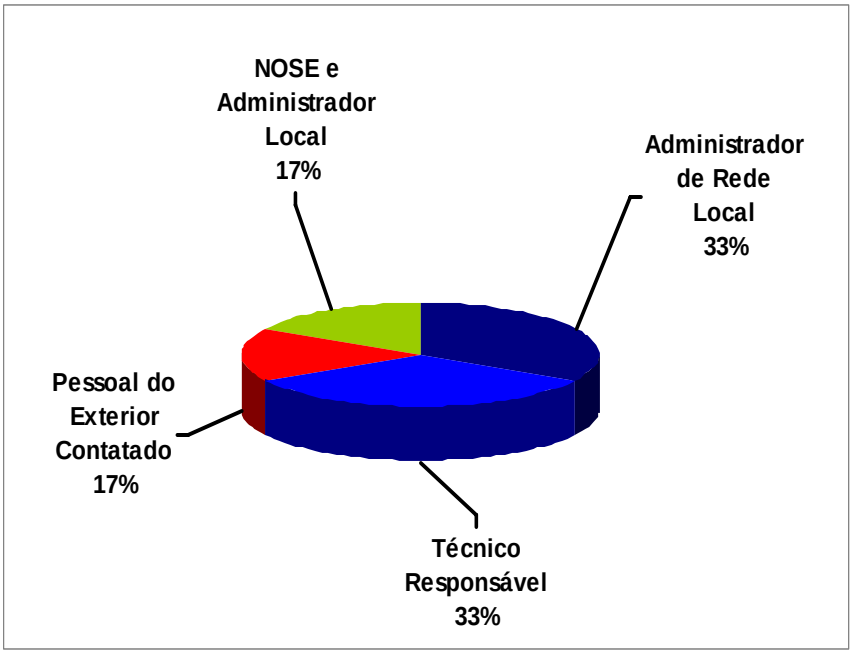
Nesta secção pretende-se mostrar, através de alguns indicadores, uma avaliação do estado da Segurança Informática nas Instituições de Ensino Superior em questão. Neste contexto, vai-se falar de aspectos como: o sistema de gestão das Redes; as práticas da segurança da informação; as políticas de segurança e auditoria postas em prática; o estado da implementação de alguns indicadores de segurança; e a sensibilidade dos inquiridos em relação à utilização das tecnologias de informação e comunicação e à segurança da informação.

5.3.2.1 O Sistema de Gestão das Redes

Os resultados obtidos em relação ao Sistema de Gestão das Redes estão representados no gráfico 6. Os resultados obtidos neste gráfico mostram que 33% das redes tem um administrador com formação de base em informática e que trabalha a tempo inteiro na instituição, 17% são administradores mas com pouca independência por ter algum apoio do

NOSE, 33% são geridas por técnicos designados para fazer este trabalho e finalmente 17% contratam pessoas fora da instituição para fazer a gestão das suas redes.

Gráfico 6 - Pessoal de Administração e Gestão das Redes



Esse e outros indicadores que serão apontados demonstram a necessidade de actualização de certos conhecimentos técnicos por parte dos administradores e uma maior sensibilização dos dirigentes em relação a aspectos sensíveis da utilização das novas tecnologias.

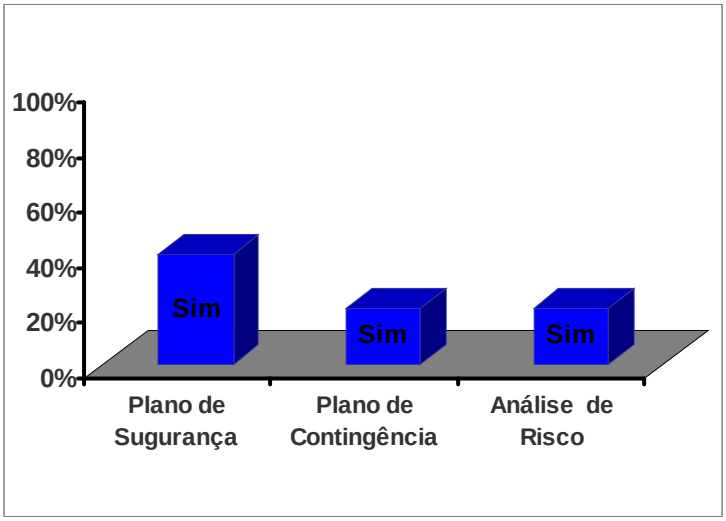
Para fazer um trabalho com este grau de responsabilidade – A gestão da Informação Institucional, não se afigura ser «boa prática» uma instituição do ensino superior contratar pessoas que não trabalham a tempo inteiro para fazer a gestão de conteúdos em formato digital tendo em conta que ali existem informações que podem ser sensíveis.

Para inverter esta situação, no sentido de instaurar uma «boa prática» de segurança institucional, defendemos, de forma crítica, a inversão da referida situação, já que, como podemos verificar, o nível de segurança é muito baixo.

5.3.2.2 Práticas da segurança e Auditoria da informação.

Ter Tecnologias de Informação e Comunicação – (TIC), dentro duma organização facilita os processos de gestão, tendo em vista que é um factor importante para a produtividade. Mas caso não forem bem geridas ao nível da segurança podem constituir-se em recursos muito perigosos à segurança da informação institucional. Nesta secção serão apresentados indicadores que avaliam o estado da segurança e auditoria dessas redes através do gráfico 7.

Gráfico 7 - Estado da Segurança Global das Instituições



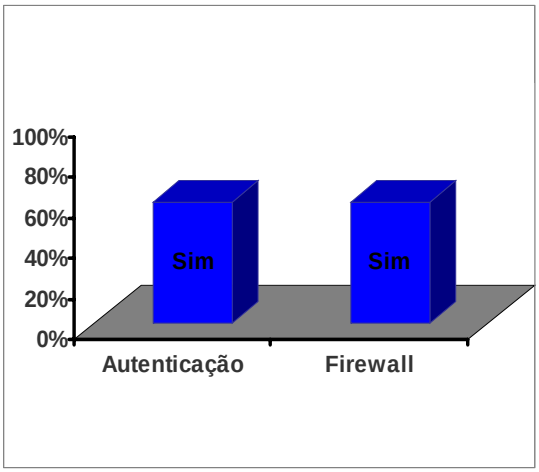
Os resultados do gráfico, indicam que a segurança nas instituições de Ensino Superior em Cabo Verde devem ser aperfeiçoadas consideravelmente porque existem aspectos muito importantes da segurança como o plano da segurança, de contingência e a análise de risco que não estão a ser levadas em consideração com o devido rigor.

A indicação da implementação de algumas práticas importantes da segurança mostra que 60% das instituições não tem um plano de segurança para a organização, o que significa que implementam soluções sem nenhum estudo prévio. No mesmo gráfico pode-se constatar que 80% das instituições não dispõem de um plano de contingência para possíveis situações de emergências, nem da análise de risco em relação às tecnologias que dispõem para avaliar perda ou ganho dos investimentos realizados.

Com esses indicadores, pode-se afirmar que as instituições de ensino superior Cabo-verdiana não têm levado em consideração os recursos financeiros que podem desperdiçar ou ganhar quando investem numa tecnologia, nem o quanto podem perder em casos de emergência por não deterem um plano de segurança e contingência, e nem possuírem uma análise de risco dos investimentos realizados.

Mas, uma instituição pode não ter um plano global de segurança e mesmo assim conservar algum índice de segurança se tiver em linha de conta aspectos como o controlo e gestão de acessos. Os resultados apresentados no gráfico 8 mostram indicadores interessantes neste aspecto.

Gráfico 8 - Controlo e Gestão de Acesso



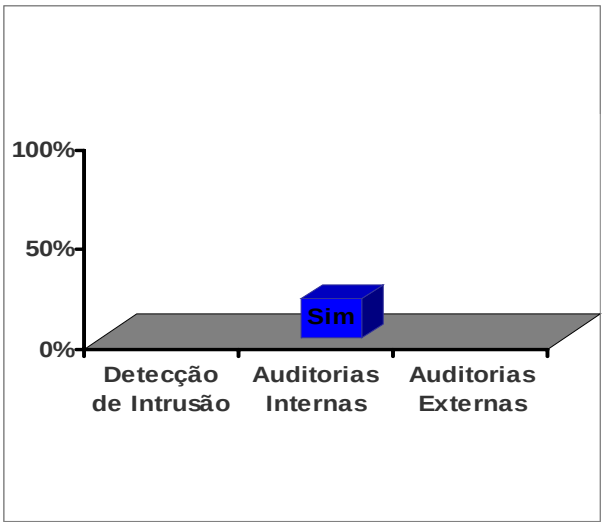
Neste gráfico pode-se observar que 60% das instituições levam em consideração a autenticação dos utilizadores e as vantagens da existência do *firewall*, o que constitui num indicador aceitável e que precisa de ser melhorado.

Estes indicadores mostram que apesar da inexistência de planos de segurança nessas instituições, estas se preocupam com a questão da segurança ao controlarem o acesso não autorizado.

Em relação à auditoria informática dessas redes, os resultados obtidos estão representados no gráfico 9. Esses resultados mostram que 100% das instituições não dispõem de um sistema de detecção de intrusões, o que significa que, por exemplo, se alguém aceder as suas redes eles não terão mecanismos de registo dessa ocorrência.

Em relação à auditoria interna, 20% dessas instituições é que fazem alguma auditoria interna para o controlo interno da rede e 100% delas nunca fizeram a auditoria externa para saberem o estado da segurança das suas redes.

Gráfico 9 - Auditoria das Redes



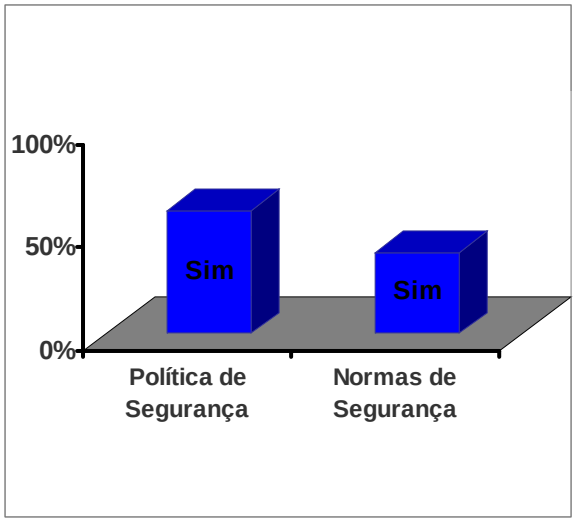
Os sistemas de detecção de intrusões de intrusões e as auditorias são aspectos importantes para avaliar o nível da vulnerabilidade duma rede local. Neste âmbito, aconselha-se essas instituições a adoptarem urgentemente estas práticas, principalmente os sistemas de detecção de intrusão com o propósito de conhecer as suas redes, a nível de falhas e vulnerabilidades, para uma possível medida correctiva.

5.3.2.3 Implementação das Políticas de Segurança

Levando em consideração que as Políticas de Segurança, constituem num conjunto de normas e procedimentos que visam proteger as organizações de possíveis ameaças, todas as organizações que utilizam meios tecnológicos sentem necessidade de implementar algumas normas, mesmo que não tendo a consciência clara da sua real importância, com o intuito de proteger os bens da organização.

Segundo os resultados obtidos no gráfico 10, observou-se que 60% das instituições tem políticas de segurança definida e 40% tem normas para a segurança da organização.

Gráfico 10 - Políticas de segurança



Os indicadores registados neste gráfico mostram que a segurança nessas organizações representa algum índice de preocupação, por isso teve-se a necessidade de analisar outros indicadores para analisar o real estado da implementação de algumas políticas de segurança. Estes estão representados na tabela 5.

Tabela 5 - Implementação de algumas políticas de segurança

Políticas de Segurança	Estado da Implementação			
	Implementado	Em Desenvolvimento	Projectado	Não considerado
Utilização dos Recursos da Instituição	80%		20%	
Sistema de controlo de Acesso	60%	40%		
Segurança no Acesso à Internet	40%	20%		40%
Segurança dos dados	60%	20%		20%
Segurança dos postos de trabalho	60%	40%		
Segurança nas instalações físicas	60%		20%	20%
Gestão das *passwords*	100%			
Responsabilização dos utilizadores	20%	20%		60%
Temporização do terminal		40%	40%	20%
Política de acesso aos recursos	40%	20%	40%	

Os indicadores da tabela 5, permitem constatar o nível da implementação de algumas políticas de segurança.

No que diz respeito à utilização dos recursos, 80% das instituições acham que os seus bens estão protegidos contra uma possível destruição pela existência de normas que protegem estes bens.

Em relação à segurança da informação no acesso a Internet, 40% das instituições dispõem da implementação de sistemas de protecção, e no que concerne à protecção dos dados, 60% já tem implementado a segurança no acesso aos dados.

No que diz respeito aos controlo de acesso, 60% das instituições tem implementado o controlo de acesso aos dados, 100% tem implementado sistema de gestão das *passwords*. Quanto à gestão da temporização dos terminais, esta não se encontra implementada em nenhuma das instituições, sendo que apenas 20% das instituições tem este aspecto em desenvolvimento, 40% tem-no projectado e 20% não considera este aspecto.

Em relação à política de acesso aos recursos da rede local, 40% das instituições consideram que já tem este item implementado.

Estes indicadores mostram que a segurança lógica dessas instituições está num nível aceitável mas ainda falta muito por fazer dado que a taxa de implementação de alguns indicadores se encontram num patamar abaixo do aceitável.

Em relação à segurança física 60% das instituições tem implementado políticas no acesso às instalações das mesmas e nos postos de trabalho. Tendo em conta que a segurança física é muito importante para garantir a segurança lógica e da informação, estas organizações devem apostar ainda mais neste tipo de segurança.

5.3.2.4 Estado da implementação de Algumas Práticas para a Segurança.

Garantir a segurança organizacional não é só implementar políticas de segurança, é também necessário fazer a manutenção das políticas definidas à medida que são adoptadas novas tecnologias para a instituição ou à medida que mudam as exigências dos utilizadores.

A tabela 6 mostra a percentagem de implementação de algumas práticas de segurança nas redes em questão, em relação a alguns serviços considerados mais comuns em redes universitárias.

Tabela 6 - Implementação de algumas práticas de Segurança

Práticas de Segurança	Estado da Implementação			
	Implementado	Em Desenvolvimento	Projectado	Não considerado
Backup/cópia de segurança centralizado	100%			
Firewall implementado	60%			40%
VPN para acesso remoto		20%		80%
Acesso a redes sem fio		20%	20%	60%
Detecção de intrusão (I.D.S)				100%
Utilização de ferramentas de I.D.S			20%	80%
Gestão dos utilizadores	100%			
Implementação de VLAN		20%		80%
Controlo de acesso físico	60%			40%
Controlo de acesso à utilização do Sistema	100%			

Em relação às práticas de segurança, pode-se observar na tabela que alguns itens têm o estatuto de excelente, outros de aceitável e de pouco aceitável em termos da sua implementação.

No nível «excelente» se destacam o *backup* (cópia de segurança) centralizado, a gestão de utilizadores e o controle de acesso ao sistema, tendo 100% das instituições esses serviços implementados. Estes indicadores mostram que a segurança nessas instituições é um aspecto considerado importante. A gestão de utilizadores, que permite o controlo do acesso ao sistema, mostra visivelmente que em nenhuma dessas redes existe acesso não autorizado através de contas de utilizadores. E em relação ao *backup* centralizado, o resultados mostram que em todas as instituições preocupam-se com a segurança da informação no que concerne à perda ou extravio da mesma.

Os que estão num nível «aceitável» destacam-se o *Firewall* e o controlo do acesso físico, com 60% de implementação nas instituições.

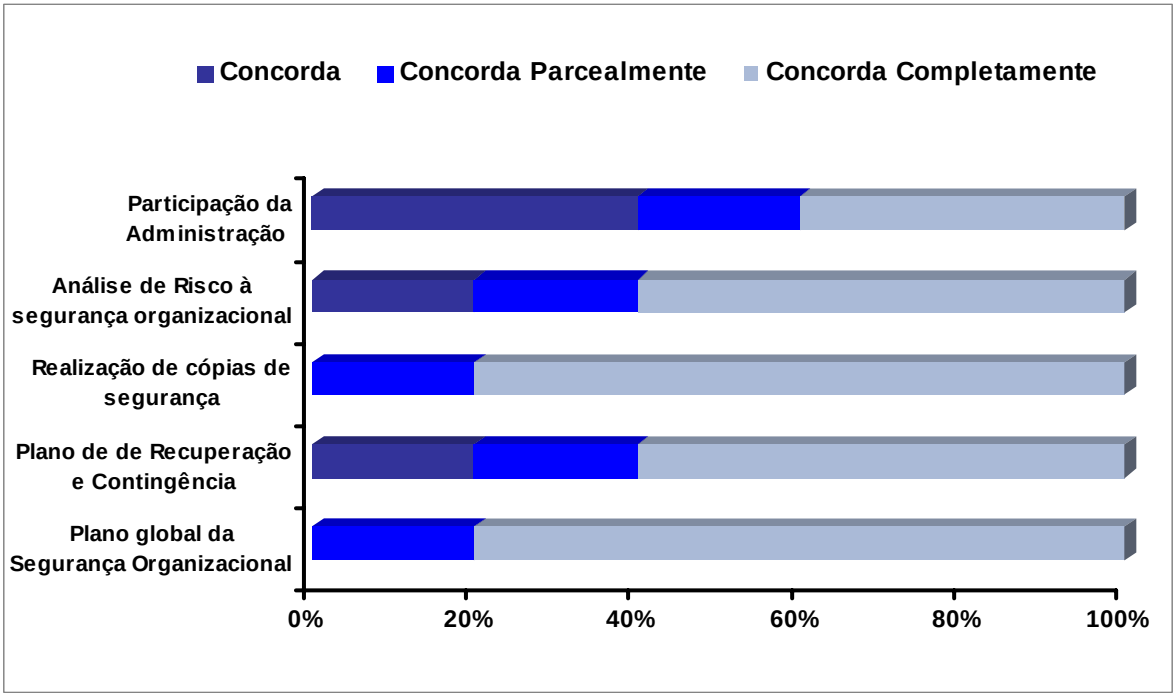
No nível «pouco aceitável» estão: A implementação de VLANS e VPNs, os sistemas de detecção de intrusão, onde a maioria das instituições não conferem importância a estes serviços, pois estes não estão incluídos nos seus planos futuros.

A leitura que se pode fazer aqui é de que existem alguns itens que estão bem implementados e outros que carecem de alguma atenção. Mas ao olharmos para os requisitos de algumas destas redes pode-se constatar que a sua falta ainda não se faz sentir, embora em cenários diferentes as exigências talvez seriam outras, por exemplo necessidade de ter esses requisitos.

5.3.2.5 Sensibilidade em relação à utilização das TICs e à Segurança da Informação.

Embora o nível de implementação da segurança não esteja num nível excelente, os administradores de redes das instituições inquiridas estão sensibilizados sobre a relevância da segurança da informação. O resultado da análise neste aspecto encontra-se no gráfico 11.

Gráfico 11 - Nível da sensibilidade dos administradores sobre a segurança



As observações que se pode fazer neste gráfico é de que 80% dos inquiridos estão totalmente de acordo que um plano de segurança é muito importante para optimizar a gestão

da rede, 60% estão sensibilizados sobre a relevância do plano de recuperação e contingência em casos de emergência, 80% se encontram sensibilizados e fazem a realização de cópias de segurança, 60% concordam totalmente que a análise de risco ajuda a organização a saber o nível de perda e de ganho de um investimento e, finalmente, apenas 40% dos inquiridos concordam inteiramente que a participação da administração ajuda na implementação de qualquer solução e/ou decisão.

Esses dados constituem num indicador muito positivo, porque embora essas instituições não têm um plano de segurança, eles tem a consciência de que esses requisitos são importantes para a segurança organizacional.

5.3.2.6 Que Perspectivas de Inovações Tecnológicas

Em relação à Inovação Tecnológica, os resultados mostram que 80% das instituições não tem um plano de utilização de tecnologias, de modo que fazem a aquisição e a actualização de tecnologias quando houver necessidade

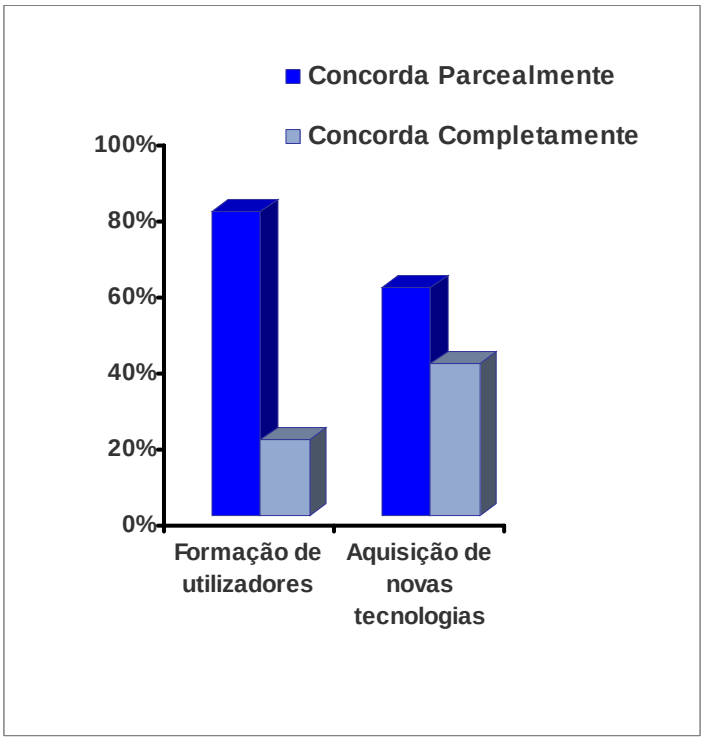
Tabela 7 - Inovação Tecnológica

Inovação Tecnológica			
Todos os anos	**2 anos**	**5 anos**	**Quando houver necessidade**
20%			80%

Um dos motivos que estão na base desses dados, segundo algumas interacções com os inqueridos realizadas, é a falta de meios financeiros.

Embora a prática de actualização dos recursos não tenha um tempo determinado em nenhuma das instituições inquiridas, e o nível de competência dos utilizadores não estar num patamar excelente, os administradores de redes demonstram alguma sensibilidade nesta questão. Segundo os dados recolhidos no estudos e apresentados no gráfico 12, 80% dos inquiridos estão parcialmente de acordo que a formação dos utilizadores é importante para uma maior rentabilização e aproveitamento dos recursos da rede e apenas 40% concorda inteiramente que a aquisição de novas tecnologias é importante num ambiente académico.

Gráfico 12 - Sensibilidades em relação à formação de utilizadores e novas tecnologias



5.3.3 Desafios e Potencialidades

No cômputo geral pode-se afirmar que as redes das instituições do Ensino Superior em Cabo Verde, estão a trilhar os caminhos para o seu desenvolvimento mas que, neste percurso, é preciso um esforço maior, principalmente no que diz respeito à aposta em inovações, porque embora em todas as instituições existam recursos disponibilizados na rede, como, por exemplo, computador, serviços de acesso à impressão, acesso à Internet e muitos outros, ainda existe muita deficiência em termos de tecnologias que podem facilitar o ensino como, por exemplo: bibliotecas digitais, sistemas de informação académica, ensino à distância e portal académico.

Para avaliar qualquer indicador é necessário conhecer a avaliação do publico alvo e, nessa óptica, algumas perguntas foram reservadas para a classificação do público, nomeadamente indicadores como a cultura organizacional para as novas tecnologias, condições de acesso para estudantes, a segurança informática e muitos outros, tendo em conta que em qualquer

estudo interessa também a opinião das pessoas em relação a alguns aspectos. Os resultados destes indicadores estão apresentados na tabela 8.

Tabela 8 - Avaliação de alguns indicadores por parte dos inquiridos

Utilização	Percentagem ...			
	Insatisfatório	Pouco satisfatório	Satisfatório	Excelente
Infra-Estrutura de Rede adequada		20%	80%	
Cultura organizacional para o aceso às novas tecnologias		20%	80%	
Sensibilidades dos dirigentes para novas soluções		20%	80%	
Corpo Docente capaz de manipular novas ferramentas e tecnologias		20%	80%	
Condições acesso aos estudantes		20%	80%	
Acesso a Laboratórios informáticos pelos estudantes		40%	60%	
Preocupação com a segurança dos dados		40%	60%	
Políticas de formação e actualização de conhecimentos		100%		

Segundo os dados na tabela, quase todos os itens estão num nível satisfatório tendo a percentagem de 80%, restando somente a política de formação de utilizadores que 100% dos inquiridos consideram que se encontra num nível pouco satisfatório, sinal que estes gostariam de poder ter mais formações a nível da utilização e implementação de novas tecnologias.

Abordando as potencialidades das instituições estudadas, considera-se que elas se encontram num patamar razoável tendo por base o facto de em todas as instituições existirem infra-estruturas de TIC modernas, pessoas sensibilizadas e algum interesse na obtenção de melhorias. Trata-se de um indicador muito positivo porque nota-se que todas as tecnologias de ensino que não existem nestas instituições mas, são relativamente fáceis de implementar, desde que existem e sejam disponibilizados meios para tal.

Conclusão

Apesar de existirem inúmeras diferenças culturais, económicas ou mesmo estruturais entre as universidades, elas têm as mesmas funções: o ensino, a investigação e a extensão universitária.

A composição orgânica das universidades, depende de alguns factores nomeadamente o país onde está instalado, condições financeiras ou mesmo anos de existência. Todas elas têm uma comunidade de alunos, docentes e funcionários e este requisito faz com que as universidades tenham nos seus organigramas serviços administrativos e académicos. Isto implica que as elas tenham docentes de várias categorias e áreas científicas, alunos de vários cursos e funcionários com diversas funções e de diferentes unidades organizacionais, tornando a universidade num espaço onde existem pessoas com perfis e funções diferentes, influenciado assim na estrutura e nos requisitos das redes universitárias.

A evolução das tecnologias de informação e de comunicação aliada aos impactos resultantes da sociedade do conhecimento estão a determinar um novo paradigma de aprendizagem trazendo consigo, exigências de actualizações e reciclagem de novos conhecimentos tanto na camada jovem como na de adultos e um novo modelo pedagógico.

Este novo paradigma, traz uma nova forma da relação e convivência professor-aluno, o professor deixa de ser a fonte absoluta de saber e transforma num incentivador de conhecimentos, alguém que promove a interacção e partilha de saberes entre participantes, indicando fontes necessárias para encontrarem subsídios de modo a construírem os seus próprios conhecimentos.

Essas mudanças tecnológicas implicam que as instituições de Ensino Superior se adaptem a essa nova realidade, uma vez que as tecnologias de informação e comunicação têm, actualmente, um papel determinante em todos os aspectos de vida organizacional, tornando-se numa ferramenta básica para o processo de ensino e aprendizagem. Para a adaptação a essas novas tecnologias, as universidades precisam de meios tecnológicos que suportem essas exigências, nomeadamente uma infra estrutura de rede adequada, a capacitação de técnicos de rede de modo a responder as exigências colocadas e a capacitação dos docentes e alunos de modo a tirarem o maior proveito possível dos recursos que lhes são disponibilizados.

A utilização dessas novas tecnologias influenciam a estrutura da rede universitária, porque todos os dias aparecem inovações, que muitas vezes são criadas pela própria universidade, devido aos constantes desafios que encontram no seio da comunidade académica. Sendo uma instituição de formação, investigação e, sobretudo, de produção de novos conhecimentos científicos, não se pode limitar nem padronizar a utilização de um determinado tipo de *hardware* e/ou *software*, razão pela qual, nas redes universitárias, encontramos uma grande heterogeneidade de tecnologias a nível de serviços, sistemas operativos, e o facto de um utilizador ter preferência por uma determinada tecnologia, não justifica o não acesso a recursos a que tem direito, cabendo, neste caso, à universidade criar e implementar soluções mais adequadas à sua realidade.

Uma das formas de solucionar este problema é criação de perfil de utilizadores onde os utilizadores têm exactamente aquilo que precisam para trabalhar e, a implementação de tecnologias de redes que facilitem o acesso aos recursos dentro e de fora da Universidade.

Mas a disponibilização desses recursos implica uma atenção especial à segurança das informações uma vez que esta é o principal suporte das universidades, porque o valor de universidade reside nos conhecimentos e nas informações que oferece.

No caso de Cabo Verde, segundo alguns indicadores, a tendência na utilização das Tecnologias de Informação e Comunicação nas instituições de ensino superior está num nível muito satisfatório, uma vez que 100% das instituições de ensino superior em Cabo Verde tem infra-estrutura de redes com acesso à Internet.

Isto constitui um indicador muito positivo, tendo em conta que a Internet permite acesso a informações ultrapassando todos os limites geográficos e temporais, para toda a comunidade académica dessas instituições e, tendo em conta que o Ensino Superior em Cabo Verde é um fenómeno muito recente, o acesso a Internet minimiza os problemas de insuficiências bibliográficas devido a existência de relativamente pouca produção científica disponível nas bibliotecas “tradicionais”.

Em relação às infra-estruturas de redes nessas instituições, existem alguns indicadores positivos em termos de recursos existentes apesar de existir algumas insuficiências a nível de inovações tecnológicas. Segundo os resultados obtidos no estudo, apesar de 100% das instituições terem redes e acesso à Internet, existem algumas insuficiências em relação às tecnologias de redes, uma vez que as redes locais sem fio (***WLAN***), constituem apenas 20% e funcionando apenas no interior do edifício sem possibilidades de acesso nas cantinas ou bibliotecas. No que diz respeito a VPN e VLAN nenhuma das instituições tem estas tecnologias, o que demostra claramente algumas insuficiências em relação a inovações tecnológicas, levando em consideração que essas tecnologias permitem algumas vantagens em relação à gestão de acesso dos utilizadores na rede universitária.

Em relação às exigência de larguras de banda, concluiu-se que a maior parte das instituições não têm exigência de grandes quantidades de largura de manda, para o acesso à Internet. Segundo os dados do estudo realizado, em 50% das instituições não existem serviços e/ou requisitos que exigem muita largura de banda, e pelo número de utilizadores e computadores

que têm, afirma-se que a maior parte dos utilizadores não utilizam serviços que exigem muita largura de banda. Um outro indicador em relação a esse aspecto é que as linhas mais utilizadas são o ADSL com 37% e o ISDN com 49,5%, para ligação à Internet.

Em relação às características de tecnologias que utilizam, pode-se afirmar que estão num nível satisfatório, uma vez que os computadores e servidores que utilizam são considerados razoáveis e os sistemas operativos são as versões mais recentes da *microsoft*. Segundos os resultados do estudo, o número de computadores existentes nessas instituições, variam de 50 a 200, e 80% são considerados como eficientes e/ou rápidos, tendo, em 90,8%, como sistema operativo de utilização diária o *microsoft Windows* 2000 *professional e XP* para um número de utilizadores que varia entre 100 a 3.000. Em relação ao número de servidores os resultados confirmam que variam de 1 a 4 representando 80% das instituições, onde 100% são servidores de dados.

Em relação a Acesso aos Recursos nas redes está num nível aceitável, segundo os resultado obtidos, porque em todas as instituições todos os funcionários têm a possibilidade de terem uma conta de utilizador e utilizar os recursos da rede. Os resultados alcançados do estudo apontam que 80% das instituições assumem que um número significativos de utilizadores tem acesso ao computador e no que diz respeita à utilização dos recursos disponibilizados na rede, 60% das instituições assumem que um número significativos de utilizadores tem acesso a computadores para efectuarem as suas tarefas e para acesso à Internet e correio electrónico. No entanto, 60% das instituições afirmam que alguns utilizadores é que conseguem aproveitar desses recursos uma vez que existe uma grande percentagem de utilizados inexperiente ou que têm alguma dificuldade.

Não basta ter tecnologias numa organização, o mais importante é saber utilizá-las e tirar o bom proveito das vantagens que podem oferecer. Os resultados da pesquisa em relação à utilização dos recursos existentes e disponibilizados nessas instituições através da rede, revelam que existe um grande défice em relação à utilização dos recursos e ao aproveitamento dos investimentos realizados, porque quando se investe numa tecnologia é necessário tirar o máximo de proveito dela, uma vez que passado algum tempo, será

considerado ultrapassado por outras novas que surgem. Os dados relativos à competência dos utilizadores nas instituições de ensino em Cabo Verde, apontam que 19% dos utilizados são inexperientes, 38% apresentam alguma dificuldade, 28% são razoáveis e 14,4% são competentes. Este resultado, constitui-se num indicador muito preocupante tendo em conta que mais de 50% não têm competências para manipular ferramentas básicas. Isto deve-se constituir num factor de preocupação e resolução por parte dos dirigentes, uma vez que a utilização das tecnologias de informação no ensino superior constituem num factor cada vez mais importante para a qualidade de ensino devido às vantagens que oferece.

No que diz respeito a tarefas que utilizadores executam no computador, os dados apontam que 100% das instituições responderam que alguns é que têm acesso a base de dados, 80% responderam que um número significativo de utilizadores utilizam as ferramentas do Microsoft *office*, e 40% responderam que um número significativo de utilizadores tem acesso a serviços de impressão. Relativamente ao aproveitamentos dos recursos da Internet, 60% das instituições responderam que somente alguns é que tiram o proveito deste recurso.

Esses dados apontam que os utilizadores precisam de mais formações e que é preciso uma maior cultura científica por parte das organizações no sentido da utilização de novas tecnologias, uma vez que 19% das instituições assumem que os seus utilizadores são inexperientes.

Em relação ao funcionamento destas universidades a grande maioria funciona de forma «tradicional», cerca de 60%, uma vez que não apresentam características aderentes a universidade digital ou virtual. Os fundamentos dessa afirmação é a inexistência, actualmente, de alguns serviços comuns às universidades, nomeadamente sistemas de informação académica, bibliotecas digitais ou o portal universitário, que são alguns serviços inerentes às universidades que funcionam de forma digital e/ou virtual.

No que diz respeito à segurança da informação, as instituições de ensino superior Cabo-verdianas, encontram-se num nível pouco satisfatório. Essa afirmação adveio da inexistência de algumas práticas importantes de segurança. Em informática quando um serviço não está operacional é como se não existisse, pois apesar de existirem alguns indicadores interessantes

em relação a certos aspectos da segurança, considera-se que a segurança nestas instituições merece uma maior atenção por parte dos administradores de redes.

Os resultados, que permitem fazer essas afirmações são os seguintes:

- Apenas 33% dos administradores de rede que trabalham a tempo inteiro como administradores e que têm formação de base para tal.
- Em 60% das instituições não existem planos de segurança nem análise de risco dos investimentos realizados.
- Em 60% das instituições não existe *firewall* implementado e operacional.
- Em 80% das instituições não é feita a auditorias interna nas redes e não levam em consideração este aspecto para possíveis melhorias.
- Em relação a políticas e normas de segurança, 40% não têm normas e políticas de segurança,
- Em 100% das instituições não há sistemas de detecção de intrusão, sendo que este aspecto não é considerado relevante.
- 80% das instituições não consideram importante e nem têm projectado as vantagens da implementação de VLANS, para a segurança da rede lógica.

No entanto, existem alguns aspectos na política de segurança implementada em algumas instituições que merecem algum destaque embora considera-se que estes não são suficientes para garantir a segurança total de uma organização:

- Em 100% das instituições faz-se o *backup* dos dados de forma centralizada.
- Em 100% das instituições fazem a gestão das *passwords* através das contas dos utilizadores.
- Em 60% das instituições está implementado um sistema de controlo de acesso às estações de trabalho e às instalações físicas.

No que concerne à sensibilidade dos administradores de redes em relação à segurança e auditoria de redes, considera-se que se encontra num grau bastante satisfatório, porque cerca

de 80% dos administradores estão consciencializados da importância de alguns aspectos chaves para a segurança, nomeadamente a participação dos dirigentes na implementação da segurança, a importância do plano de segurança, do plano de contingência e de recuperação em casos de emergência, apesar destes não estarem implementados nas suas redes.

Concluindo, a tendência actual leva a considerar que, numa visão de médio e longo prazo, alguns aspectos podem sofrer um desenvolvimento qualitativo, como se pode evidenciar pelo facto deste presente estudo ter servido, igualmente, para despertar a atenção dos inquiridos para alguns aspectos da segurança dos sistemas de informação que até então tinham sido por eles negligenciados, como aliás manifestaram, de forma explícita, no decorrer das interacções havidas na realização do estudo.

A terminar, nenhum trabalho científico deixa o autor completamente satisfeito, todavia este estudo, que tem muito mais a desbravar, está aberto a críticas, melhorias e investigações futuras.

Bibliografia

Antunes, J. A. Castro, E. A. M. (2001). *Tecnologias de Comunicação e Informação na configuração das relações dos sujeitos*, Universidade de Aveiro. Portugal.

Aretio, G.(1994). *Education a Distancia Hoy, Madrid*. UNEP. Education a Distancia.

Melo1, A. M., Amorim J. S., Baranauskas, M. Et all. *Desafios para a Tecnologia da Informação e Comunicação em Espaço Educacional Inclusivo*. Universidade Estadual de Campinas.

Chellapa, R. Barua, A. And Whinston, A. D.: (1997). *An Electrinic Infrastructure for virtual university*, communications of the ACM 40(9), 56-58.

Cordeiro, A.(2002). *Auditoria de Sistemas de Informação*, 2ª Edição, FCA- Editora de Informática Ltda, 2002.

Cordeiro, Aberto. (2002). *Introdução à Segurança dos Sistemas de Informação*. *Segurança um de Sucesso – Auditoria e Benefícios da Segurança*, Lisboa, FCA- Editora de Informática Ltda.

Carneiro, A. (2004), *Auditoria de Sistemas de Informação,* Lisboa, FCA- Editora de Informática Ltda,

Figueiredo A. (2000), *Web-Based Learning: Largely beyond content*, Porto, FEUP Edições.

Ferreira, Jorge. (1995). *Segurança dos Sistemas de Informação*, Lisboa, Instituto de Informática ANS.

Freira, António Manuel. Damas, Luís, *Módulo de administração de Utilizadores*, Janeiro de 2002, Disponível <http://www.bibliosoft.pt/suporte/docs/bb2004-admutils.pdf > [consultado em 29 de Maio de 2005].

Fujita, M. S. L.: *Aspectos evolutivos das Bibliotecas Universitárias em Ambiente Digital na perspectiva da rede de Bibliotecas da UNSP*.
Disponível em <http://www.informacaoesociedade.ufpb.br/pdf/IS1520504.pdf>, [Consultado em 2 de junho de 2006].

Gatien, G.M.: (2000), *trust, privacy and the digital university, the technology source*. Disponível em <http://ts.mivu.org/default.asp?show=article&id=1034> [consultado a 7 de setembro de 2005].

Hai, C.B:(2005), bulding a digital campus, technical report, Sun Microsyztems. Disponível em <http//sg.sun.com/events/presentation/files/thai-erc/digital-campus.pdf> [consultado em 26 de Agosto de 2005]

Heseltine, R. and Dolphin, I.(2001), Building the Digital University, Tecnical report, The University of Hull. Disponível em <http//www.digital.hull.ac.uk/downloads/ dup-1st-Ann.pdf>,[consultado em 15 de agosto de 2005].

Holmberg, B. *Educatión a Distamcia, Situation y Perspectiva*, Boenos Aires, Editorial Kapelusz .

Franco, Hilário (2001), *Aunditorial Aontábil*, Editora Atlas

Imre Simon. (1997).*A Universidade diante das novas tecnologias de informação e comunicação*, Jornal da USP,
disponível no site <http://www.ime.usp.br/~is/abc/ > ,[consultado em 15 de Maio de 2006].

Jones, K.: 2004,2005: *the year of the digital campus, T.H.E. Journal*. Disponível em <http//www.thejournal.com/magazine/vault/a5153.cfm>,[consultado a 13 de janeiro de 2005].

KENSKI, V.M. (1998): «*A profissão do professor em um mundo em rede: exigências de hoje, tendências e construção do amanhã: professores, o futuro é hoje», em: Tecnologia Educacional*, v.26 (143), pp.65-69.

Losch, P.: 2002, *The digital campus Primeer*, Sun Microsistems.

Lindeberg, Barros. Shitserka, Ricardo. Redes de Computadores, Dados, Voz e Imagem, 6ª Edição, Editora Hérica Ltda, 2002.

Loureiro, P. (2001). *Windows 2000 Server para Profissionais*, volume 1, 3ª Edição, FCA-Editora de Informática Ltda.

Loureiro, Paulo. *Windows 2000 Server para Profissionais*, volume 2, FCA- Editora de Informática Ltda, 2001.

Noerr, P. (2003), *The Digital Library Toolkit, 3 edn*, Sun Microsystems.

Marques, M. B.; Gouveis, L. B. *Bibliotecas Digitais, A importância de Serviço de referência.* Disponível em [http://www2.ufp.pt/~lmbg/com/margarida_iadisibero04.pdf,],
Consultado a [2 de junho de 2006].

Melo, A . M.; Amorim, J. S.; Baranauskas, M. C. ; Alcoba, S. de A. C.; *Desafios para a Tecnologia da Informação e Comunicação em Espaço Educacional Inclusivo,* Universidade Estadual de Campinas. Disponível em <[http://www.dcc.unicamp.br/~melo/publicacoes/wie2005.pdf#search=%22Desafios%20para%20a%20Tecnologia%20da%20Informa%C3%A7%C3%A3o%20e%20Comunica%C3%A7%C3%A3o%20%5Bpdf%5D%22>, [consultado em 21 de setembro de 2006].

Mehlecke, Q. T.; Tourouco, L. M.: *Ambientes de Suporte para a Educação a Distância, A Medição para a aprendizagem Cooperativa,* Disponível em [http://www.cinted.ufrgs.br/renote/fev2003/artigos/querte_ambientes.pdf#search=%22ensino%20a%20dist%C3%A2ncia%20%2B%20universidades%20%5Bpdf%5D%22], consultado a 13 de Setembro de 2006.

Minasi, M. Anderson, C. Smith, B. M. Toombs, D.. *Dominando o Windows 2000 Server,* A Bíblia, Tradução e Revisão Técnica: Equipe Makon Books de Informática, São Paulo, 2001

Monteiro, E. Fernando B, *Engenharia de Redes Informáticas*, 4ª Edição,FCA- Editora de Informática Ltda, 2000

Oliveira, G. P.(2005) ; Faculdade Politécnica de Jundiaí, OEI-Revista Iberoamericana de Educación (ISSN: 1681-5653), *Novas tecnologias da informação e da comunicação e a construção do conhecomento em cursos Universitários: Reflexões sobre acesso, conexões e virtualidade,* disponível em http://www.cibera.de, [consultado a 23 de junho de 2006]

Parecer sobre o conceito de instituição do ensino superior, Concelho Nacional de Avaliação do Ensino Superior de Portugal, disponível em

[http://www.cnaves.pt/DOCS/Pareceres/parecer_conceito_instituicao_ensino_superior.pdf], Capturado em [23 de Maio de 2006].

Pienaar, Heila. (2003). *Design and Development of an Academic information Service*, University of Pretoria, South Africa, disponível em

[http://www.cnaves.pt/DOCS/Pareceres/parecer_conceito_instituicao_ensino_superior.pdf], Capturado em [23/5/06].

Peters. Otto. (2001). *Didáctica do Ensino a Distância,* São Leopoldo, RS Unisinos

PIENAAR, HEILA. *Design and Development of an Academic Portal.* Academic Information Service, University of Pretoria, South Africa, disponível em http://www.librijournal.org/pdf/2003-2pp118http://www.librijournal.org/pdf/2003-2pp11829.pdf#search=%22Academic%20Portal%20%20%5Bpdf%5D%>, [Consultado em 10 de janeiro de 2006]

Pienaar, H. 2001. Die ontwerp van ‘n Webportaal vir akademici (Design of a Web portal foracademics). University of Pretoria.Disponível em: http://hagar.up. ac.za/catts/learner/heilap/skripsie.html; [consultado a 3 de outubro, 2002]

Pienaar, H., Conradie, F. 2001. Design and development of a portal for academics. *6th Southern African online information meeting, Kempton Park, South Africa, 19–21 June 2001*. Disponível em: http://hagar.up.ac.za/catts/learner/heilap/portaalakademicilesing.ppt [consultado a 3 de outubro, 2002]

Sistemas e Tecnologias de Informação No espaço Ibérico, "Modelos Organizacionais e Sistemas de Informação" , Actas da 1ª Conferência Ibérica de Sistemas e Tecnologias de Informação, Volume 1, Ofir, Portugal 21 a 23 de Junho de 2006.

Serrano A. Caldeiro M. Guerreiro, A. (2004). *Gestão de Sistemas e Tecnologias de Informação*, FCA- Editora de Informática Ltda,

Rosa, I. B.(2005).*Contrução de uma Biblioteca Digital, "O caso da Biblioteca Digital da Unipiaget"* , Universidade Jean Piaget de Cabo Verde, Universidade de Santiago de Compostela.

Rurato, P.; Gouveia, L. B., Gouveia, J. B. *Características essenciais do Ensino a Distância*

Disponível em [http://www2.ufp.pt/~lmbg/com/eLes04%20paulorurato.pdf#search=%22ensino%20a%20dist%C3%A2ncia%20%5Bpdf%5D%22] consultado a 13 de setembro de 2006.

Kléber, R. Segurança Segurança da Informação nas Universidades A Experiência da UFRN. Universiidade Federall do Rio Grande do Norte.

Revista Científica contacto, Universidade Jean Piaget de Cabo Verde, ,1ª Edição

RIÇO M. (2002), *O ensino profissional português na sociedade do conhecimento; o novo paradigma educacional*, Dissertação de Mestrados, Porto.

Rodrigues, V. M. T.(2004) *As tecnologias de informação e comunicação no ensino da demografia*, Universidade do Minho, disponível em <http://www.apdemografia.pt>, capturado[23/6/06]

Rodrigues, L. S. (2002). *Arquitectura dos Sistemas de Informação*, FCA- Editora de Informática Ltda,

Tecnologias de Informação: Soluções e Desafios, Revista FAE Business, nº 6, Agosto 2003, disponível em

http://www.fae.edu/publicacoes/pdf/revista_fae_business/n6/entrevista_tisolucoesedesafios.pdf>,[consultado em 10 de setembro de 2006]

Taylor, James Clifford (2006), *Palestra no X Congresso Internacional de Educação a Distância*, Universidade de Southern Queensland, Austrália 1/ 10/2003
Disponível em http://www.universia.com.br/html/materia/materia_ccch.html, [consultado em 17 de Agosto de 2006]

Varajão, J. E. Q. (1998). *Arquitectura da Gestão dos Sistemas de Informação*, 2ª Edição, Lisboa, FCA- Editora de Informática Ltda,

Manuel de utilizador do sistema de gestão de utilizadores,(2005) Instituto Informática, http://www.bdap.minfinancas.pt/documentos/manualutilizador_SGUv1.1.pdf [capturado em 7de Abril de 2005].

É o fim da Universidade tradicional, Palestra no X Congresso Internacional de Educação a Distância, fala sobre as mudanças exigidas pela universidade, Publicado em 01/10/2003 - 13:33 disponível em
http://www.universia.com.br/html/materia/materia_ccch.html
Consultado a 28 de setembro de 2006

Anexos

Questionário 1

Este questionário permitiu recolher todas as informações necessárias para avaliar as tecnologias de informação e comunicação e sensibilidades dos administradores de redes, nas instituições de Ensino Superior em Cabo Verde

Questionário 2

Este questionário permitiu recolher todas as informações necessárias para avaliar a segurança informática nas instituições de Ensino Superior em Cabo Verde.